Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-5018 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-5024 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have a Heap Overflow vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-5015 SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-5022 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-5025 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-5012 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-5026 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an	2018-07-20	Aún sin calcular	CVE-2018-5016 BID SECTRACK

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.			CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have a Use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-12792 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-5070 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have a Heap Overflow vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-5028 SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-5064 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-5066 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have a Use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-5009 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-12767 BID SECTRACK CONFIRM
adobe --	Adobe Acrobat and Reader 2018.011.20040	2018-07-20	Aún sin calcular	CVE-2018-12786

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
acrobat_and_reader	and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.			BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have a Heap Overflow vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-5052 SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-12789 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-12790 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-12771 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-5063 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have a Use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-5011 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information	2018-07-20	Aún sin calcular	CVE-2018-5027 BID SECTRACK CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	disclosure.			
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-5014 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-12787 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have a Heap Overflow vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-5058 SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-5020 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-5055 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-5035 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-5056 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an	2018-07-20	Aún sin calcular	CVE-2018-5068 BID SECTRACK

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.			CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-5046 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-5048 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-5059 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have a Heap Overflow vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-12798 SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-12781 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have a Use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-12791 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have a Double Free vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-12782 BID SECTRACK CONFIRM
adobe --	Adobe Acrobat and Reader 2018.011.20040	2018-07-20	Aún sin calcular	CVE-2018-5060

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
acrobat_and_reader	and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.			BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have a Heap Overflow vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-5067 SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have a Type Confusion vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-5057 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-5033 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have a Heap Overflow vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-5032 SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-12760 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-5019 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have a Buffer Errors vulnerability. Successful exploitation could lead to arbitrary code	2018-07-20	Aún sin calcular	CVE-2018-5034 BID SECTRACK CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	execution in the context of the current user.			
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-12765 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-5047 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have a Heap Overflow vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-5045 SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-5017 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-5050 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have a Heap Overflow vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-5040 SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-5069 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have a	2018-07-20	Aún sin calcular	CVE-2018-12770 BID SECTRACK

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.			CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have a Use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-12773 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-5054 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-12768 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have a Use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-12796 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have a Use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-12772 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-5031 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-5030 BID SECTRACK CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have a Use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-12797 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-5049 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-12779 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-12803 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have a Security Bypass vulnerability. Successful exploitation could lead to privilege escalation.	2018-07-20	Aún sin calcular	CVE-2018-12802 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-5051 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have a Use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-5065 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have a Use-after-free vulnerability. Successful	2018-07-20	Aún sin calcular	CVE-2018-12783 BID SECTRACK CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	exploitation could lead to arbitrary code execution in the context of the current user.			
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have a Use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-12756 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-12754 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-5044 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have a Buffer Errors vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-12784 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have a Heap Overflow vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-12785 SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-12780 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-12795 BID SECTRACK CONFIRM
adobe -- acrobat_and_read	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and	2018-07-20	Aún sin calcular	CVE-2018-12757 BID

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
er	2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.			SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-12774 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-5053 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-12761 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-5062 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have a Type Confusion vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-12793 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have a Heap Overflow vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-12788 SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-12766 BID SECTRACK CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-12758 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-5042 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-12755 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-5061 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-12777 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have a Heap Overflow vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-5036 SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-12762 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful	2018-07-20	Aún sin calcular	CVE-2018-5029 BID SECTRACK CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	exploitation could lead to information disclosure.			
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-12763 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-5039 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have a Buffer Errors vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-5043 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have a Use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-12776 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have a Buffer Errors vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-5037 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have a Heap Overflow vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-5041 SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-12764 BID SECTRACK CONFIRM
adobe -- acrobat_and_read	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and	2018-07-20	Aún sin calcular	CVE-2018-5038 SECTRACK

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
er	2015.006.30418 and earlier versions have a Heap Overflow vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.			CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have a Type Confusion vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-12794 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-5010 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-5021 BID SECTRACK CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader 2018.011.20040 and earlier, 2017.011.30080 and earlier, and 2015.006.30418 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-5023 BID SECTRACK CONFIRM
adobe -- connect	Adobe Connect versions 9.7.5 and earlier have an Insecure Library Loading vulnerability. Successful exploitation could lead to privilege escalation.	2018-07-20	Aún sin calcular	CVE-2018-12805 BID CONFIRM
adobe -- connect	Adobe Connect versions 9.7.5 and earlier have an Authentication Bypass vulnerability. Successful exploitation could lead to session hijacking.	2018-07-20	Aún sin calcular	CVE-2018-12804 BID SECTRACK CONFIRM
adobe -- experience_manager	Adobe Experience Manager versions 6.2 and 6.3 have a Server-Side Request Forgery vulnerability. Successful exploitation could lead to sensitive information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-5004 BID CONFIRM
adobe -- experience_manager	Adobe Experience Manager versions 6.4 and earlier have a Server-Side Request Forgery vulnerability. Successful exploitation could lead to sensitive information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-5006 BID CONFIRM
adobe -- experience_man	Adobe Experience Manager versions 6.4 and earlier have a Server-Side Request Forgery	2018-07-20	Aún sin calcular	CVE-2018-12809 BID

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ager	vulnerability. Successful exploitation could lead to sensitive information disclosure.			CONFIRM
adobe -- flash_player	Adobe Flash Player 30.0.0.113 and earlier versions have a Type Confusion vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.	2018-07-20	Aún sin calcular	CVE-2018-5007 BID SECTRACK REDHAT CONFIRM
adobe -- flash_player	Adobe Flash Player 30.0.0.113 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2018-07-20	Aún sin calcular	CVE-2018-5008 BID SECTRACK REDHAT CONFIRM
advancecomp -- advancecomp	An out-of-bounds heap buffer read flaw was found in the way advancecomp before 2.1-2018/02 handled processing of ZIP files. An attacker could potentially use this flaw to crash the advzip utility by tricking it into processing crafted ZIP files.	2018-07-27	Aún sin calcular	CVE-2018-1056 CONFIRM CONFIRM MLIST CONFIRM UBUNTU
ansible -- ansible	An input validation vulnerability was found in Ansible's mysql_user module before 2.2.1.0, which may fail to correctly change a password in certain circumstances. Thus the previous password would still be active when it should have been changed.	2018-07-26	Aún sin calcular	CVE-2016-8647 REDHAT CONFIRM CONFIRM
ansible -- tower	A flaw was found in Ansible Tower's interface before 3.1.5 and 3.2.0 with SCM repositories. If a Tower project (SCM repository) definition does not have the 'delete before update' flag set, an attacker with commit access to the upstream playbook source repository could create a Trojan playbook that, when executed by Tower, modifies the checked out SCM repository to add git hooks. These git hooks could, in turn, cause arbitrary command and code execution as the user Tower runs as.	2018-07-27	Aún sin calcular	CVE-2017-12148 REDHAT CONFIRM
apache -- kafka	In Apache Kafka 0.9.0.0 to 0.9.0.1, 0.10.0.0 to 0.10.2.1, 0.11.0.0 to 0.11.0.2, and 1.0.0, authenticated Kafka users may perform action reserved for the Broker via a manually created fetch request interfering with data replication, resulting in data loss.	2018-07-26	Aún sin calcular	CVE-2018-1288 MLIST
apache -- kafka	In Apache Kafka 0.10.0.0 to 0.10.2.1 and 0.11.0.0 to 0.11.0.1, authenticated Kafka clients may use impersonation via a manually crafted protocol message with	2018-07-26	Aún sin calcular	CVE-2017-12610 BID MLIST

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	SASL/PLAIN or SASL/SCRAM authentication when using the built-in PLAIN or SCRAM server implementations in Apache Kafka.			
apache -- openwhisk	In PHP Runtime for Apache OpenWhisk, a Docker action inheriting one of the Docker tags openwhisk/action-php-v7.2:1.0.0 or openwhisk/action-php-v7.1:1.0.1 (or earlier) may allow an attacker to replace the user function inside the container if the user code is vulnerable to code exploitation.	2018-07-23	Aún sin calcular	CVE-2018-11756 CONFIRM MLIST
apache -- openwhisk	In Docker Skeleton Runtime for Apache OpenWhisk, a Docker action inheriting the Docker tag openwhisk/dockerskeleton:1.3.0 (or earlier) may allow an attacker to replace the user function inside the container if the user code is vulnerable to code exploitation.	2018-07-23	Aún sin calcular	CVE-2018-11757 CONFIRM MLIST
apache -- tomee	The TomEE console (tomee-webapp) has a XSS vulnerability which could allow javascript to be executed if the user is given a malicious URL. This web application is typically used to add TomEE features to a Tomcat installation. The TomEE bundles do not ship with this application included. This issue can be mitigated by removing the application after TomEE is setup (if using the application to install TomEE), using one of the provided pre-configured bundles, or by upgrading to TomEE 7.0.5. This issue is resolve in this commit: b8bbf50c23ce97dd64f3a5d77f78f84e47579863.	2018-07-23	Aún sin calcular	CVE-2018-8031 MLIST
arm -- mbed_tls	ARM mbed TLS before 2.12.0, before 2.7.5, and before 2.1.14 allows local users to achieve partial plaintext recovery (for a CBC based ciphersuite) via a cache-based side-channel attack.	2018-07-28	Aún sin calcular	CVE-2018-0498 CONFIRM
arm -- mbed_tls	ARM mbed TLS before 2.12.0, before 2.7.5, and before 2.1.14 allows remote attackers to achieve partial plaintext recovery (for a CBC based ciphersuite) via a timing-based side-channel attack. This vulnerability exists because of an incorrect fix (with a wrong SHA-384 calculation) for CVE-2013-0169.	2018-07-28	Aún sin calcular	CVE-2018-0497 CONFIRM
asus -- hg100_devices	ASUS HG100 devices with firmware before 1.05.12 allow unauthenticated access, leading to remote command execution.	2018-07-25	Aún sin calcular	CVE-2018-11491 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
atlassian -- jira	The Webhooks component of Atlassian Jira before version 7.6.7 and from version 7.7.0 before version 7.11.0 allows remote attackers who are able to observe or otherwise intercept webhook events to learn information about changes in issues that should not be sent because they are not contained within the results of a specified JQL query.	2018-07-24	Aún sin calcular	CVE-2017-18104 CONFIRM
aubio -- aubio	An issue was discovered in aubio 0.4.6. A SEGV signal can occur in aubio_source_avcodec_readframe in io/source_avcodec.c, as demonstrated by aubiomfcc.	2018-07-23	Aún sin calcular	CVE-2018-14521 MISC
aubio -- aubio	An issue was discovered in aubio 0.4.6. A SEGV signal can occur in aubio_pitch_set_unit in pitch/pitch.c, as demonstrated by aubionotes.	2018-07-23	Aún sin calcular	CVE-2018-14522 MISC
aubio -- aubio	An issue was discovered in aubio 0.4.6. A buffer over-read can occur in new_aubio_pitchyinfft in pitch/pitchyinfft.c, as demonstrated by aubionotes.	2018-07-23	Aún sin calcular	CVE-2018-14523 MISC
aveva -- intouch	AVEVA InTouch 2014 R2 SP1 and prior, InTouch 2017, InTouch 2017 Update 1, and InTouch 2017 Update 2 allow an unauthenticated user to send a specially crafted packet that could overflow the buffer on a locale not using a dot floating point separator. Exploitation could allow remote code execution under the privileges of the InTouch View process.	2018-07-24	Aún sin calcular	CVE-2018-10628 BID MISC CONFIRM
bagecms -- bagecms	index.php?r=admini/admin/create in BageCMS V3.1.3 allows CSRF to add a background administrator account.	2018-07-24	Aún sin calcular	CVE-2018-14582 MISC
bento4 -- bento4	An issue has been discovered in Bento4 1.5.1-624. A SEGV can occur in AP4_Processor::ProcessFragments in Core/Ap4Processor.cpp.	2018-07-24	Aún sin calcular	CVE-2018-14590 MISC
bento4 -- bento4	An issue was discovered in Bento4 1.5.1-624. There is a heap-based buffer over-read in AP4_Mpeg2TsVideoSampleStream::WriteSample in Core/Ap4Mpeg2Ts.cpp after a call from Mp42Hls.cpp, a related issue to CVE-2018-13846.	2018-07-23	Aún sin calcular	CVE-2018-14532 MISC
bento4 -- bento4	An issue has been discovered in Bento4	2018-07-24	Aún sin calcular	CVE-2018-14587

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	1.5.1-624. AP4_MemoryByteStream::WritePartial in Core/Ap4ByteStream.cpp has a buffer over-read.			MISC
bento4 -- bento4	An issue was discovered in Bento4 1.5.1-624. There is an unspecified "heap-buffer-overflow" crash in the AP4_HvccAtom class in Core/Ap4HvccAtom.cpp.	2018-07-23	Aún sin calcular	CVE-2018-14531 MISC
bento4 -- bento4	An issue has been discovered in Bento4 1.5.1-624. A NULL pointer dereference can occur in AP4_DataBuffer::SetData in Core/Ap4DataBuffer.cpp.	2018-07-24	Aún sin calcular	CVE-2018-14588 MISC
bento4 -- bento4	An issue has been discovered in Bento4 1.5.1-624. AP4_Mp4AudioDsiParser::ReadBits in Codecs/Ap4Mp4AudioInfo.cpp has a heap-based buffer over-read.	2018-07-24	Aún sin calcular	CVE-2018-14589 MISC
bento4 -- bento4	There exists one NULL pointer dereference vulnerability in AP4_JsonInspector::AddField in Ap4Atom.cpp in Bento4 1.5.1-624, which can allow attackers to cause a denial-of-service via a crafted mp4 file. This vulnerability can be triggered by the executable mp4dump.	2018-07-23	Aún sin calcular	CVE-2018-14543 MISC
bento4 -- bento4	An issue has been discovered in Bento4 1.5.1-624. AP4_AvccAtom::Create in Core/Ap4AvccAtom.cpp has a heap-based buffer over-read.	2018-07-24	Aún sin calcular	CVE-2018-14584 MISC MISC
bento4 -- bento4	An issue has been discovered in Bento4 1.5.1-624. AP4_BytesToUInt16BE in Core/Ap4Utils.h has a heap-based buffer over-read after a call from the AP4_Stz2Atom class.	2018-07-24	Aún sin calcular	CVE-2018-14585 MISC
bento4 -- bento4	There exists one invalid memory read bug in AP4_SampleDescription::GetFormat() in Ap4SampleDescription.h in Bento4 1.5.1-624, which can allow attackers to cause a denial-of-service via a crafted mp4 file. This vulnerability can be triggered by the executable mp42ts.	2018-07-23	Aún sin calcular	CVE-2018-14544 MISC
bento4 -- bento4	There exists one invalid memory read bug in AP4_SampleDescription::GetType() in Ap4SampleDescription.h in Bento4 1.5.1-624, which can allow attackers to cause a denial-of-service via a crafted mp4 file. This vulnerability can be triggered by the	2018-07-23	Aún sin calcular	CVE-2018-14545 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	executable mp42ts.			
bento4 -- bento4	An issue has been discovered in Bento4 1.5.1-624. A SEGV can occur in AP4_Mpeg2TsAudioSampleStream::WriteSample in Core/Ap4Mpeg2Ts.cpp, a different vulnerability than CVE-2018-14532.	2018-07-24	Aún sin calcular	CVE-2018-14586 MISC
brynamics -- online_trade	Brynamics "Online Trade - Online trading and cryptocurrency investment system" allows remote attackers to obtain sensitive information via a direct request for /dashboard/addplan, /dashboard/paywithcard/charge, /dashboard/withdrawal, or /privacy&terms, as demonstrated by reading database username, database password, database_name, and IP address fields, related to CVE-2018-12908.	2018-07-23	Aún sin calcular	CVE-2018-14328 MISC
busybox -- busybox	huft_build in archival/libarchive/decompress_gunzip.c in BusyBox before 1.27.2 misuses a pointer, causing segfaults and an application crash during an unzip operation on a specially crafted ZIP file.	2018-07-26	Aún sin calcular	CVE-2015-9261 MISC MISC MISC MLIST
calamp -- lmu_3030_series_devices	CalAmp LMU 3030 series OBD-II CDMA and GSM devices has an SMS (text message) interface that can be deployed where no password is configured for this interface by the integrator / reseller. This interface must be password protected, otherwise, the attacker only needs to know the phone number of the device (via an IMSI Catcher, for example) to send administrative commands to the device. These commands can be used to provide ongoing, real-time access to the device and can configure parameters such as IP addresses, firewall rules, and passwords.	2018-07-24	Aún sin calcular	CVE-2017-3217 CERT-VN BID
ceph -- ceph	In Ceph, a format string flaw was found in the way libradosstriper parses input from user. A user could crash an application or service using the libradosstriper library.	2018-07-27	Aún sin calcular	CVE-2017-7519 BID CONFIRM
chamanet -- memocgi	Directory traversal vulnerability in ChamaNet MemoCGI v2.1800 to v2.2200 allows remote attackers to read arbitrary files via unspecified vectors.	2018-07-26	Aún sin calcular	CVE-2018-0617 JVN CONFIRM
chamilo --	Chamilo LMS version 11.x contains an	2018-07-23	Aún sin calcular	CVE-2018-1999019

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
chamilo-lms	Unserialization vulnerability in the "hash" GET parameter for the api endpoint located at /webservices/api/v2.php that can result in Unauthenticated remote code execution. This attack appear to be exploitable via a simple GET request to the api endpoint. This vulnerability appears to have been fixed in After commit 0de84700648f098c1fbf6b807dee28ec640ef e62.			CONFIRM MISC
cloud_foundry_foundation -- uaa	Cloud Foundry UAA, versions 4.19 prior to 4.19.2 and 4.12 prior to 4.12.4 and 4.10 prior to 4.10.2 and 4.7 prior to 4.7.6 and 4.5 prior to 4.5.7, incorrectly authorizes requests to admin endpoints by accepting a valid refresh token in lieu of an access token. Refresh tokens by design have a longer expiration time than access tokens, allowing the possessor of a refresh token to authenticate longer than expected. This affects the administrative endpoints of the UAA. i.e. /Users, /Groups, etc. However, if the user has been deleted or had groups removed, or the client was deleted, the refresh token will no longer be valid.	2018-07-24	Aún sin calcular	CVE-2018-11047 CONFIRM
cthackers -- adm-zip	adm-zip npm library before 0.4.9 is vulnerable to directory traversal, allowing attackers to write to arbitrary files via a ../ (dot dot slash) in a Zip archive entry that is mishandled during extraction. This vulnerability is also known as 'Zip-Slip'.	2018-07-25	Aún sin calcular	CVE-2018-1002204 CONFIRM CONFIRM MISC MISC MISC
curl -- curl	curl before 7.53.0 has an incorrect TLS Certificate Status Request extension feature that asks for a fresh proof of the server's certificate's validity in the code that checks for a test success or failure. It ends up always thinking there's valid proof, even when there is none or if the server doesn't support the TLS extension in question. This could lead to users not detecting when a server's certificate goes invalid or otherwise be mislead that the server is in a better shape than it is in reality. This flaw also exists in the command line tool (--cert-status).	2018-07-27	Aún sin calcular	CVE-2017-2629 BID SECTRACK CONFIRM CONFIRM GENTOO CONFIRM
cybozu -- cybozu_garoon	SQL injection vulnerability in the Notifications application in the Cybozu	2018-07-26	Aún sin calcular	CVE-2018-0607 JVN

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Garoon 3.5.0 to 4.6.2 allows remote authenticated attackers to execute arbitrary SQL commands via unspecified vectors.			CONFIRM
dahua_security -- ip_camera_products	Dahua IP camera products using firmware versions prior to V2.400.0000.14.R.20170713 include a version of the Sonia web interface that may be vulnerable to a stack buffer overflow. Dahua IP camera products include an application known as Sonia (/usr/bin/sonia) that provides the web interface and other services for controlling the IP camera remotely. Versions of Sonia included in firmware versions prior to DH_IPC-Consumer-Zi-Themis_Eng_P_V2.408.0000.11.R.20170621 do not validate input data length for the 'password' field of the web interface. A remote, unauthenticated attacker may submit a crafted POST request to the IP camera's Sonia web interface that may lead to out-of-bounds memory operations and loss of availability or remote code execution. The issue was originally identified by the researcher in firmware version DH_IPC-HX1X2X-Themis_EngSpnFrn_N_V2.400.0000.30.R.20160803.	2018-07-24	Aún sin calcular	CVE-2017-3223 BID CERT-VN
dbpower -- dbpower	The DBPOWER U818A WIFI quadcopter drone provides FTP access over its own local access point, and allows full file permissions to the anonymous user. The DBPower U818A WIFI quadcopter drone runs an FTP server that by default allows anonymous access without a password, and provides full filesystem read/write permissions to the anonymous user. A remote user within range of the open access point on the drone may utilize the anonymous user of the FTP server to read arbitrary files, such as images and video recorded by the device, or to replace system files such as /etc/shadow to gain further access to the device. Furthermore, the DBPOWER U818A WIFI quadcopter drone uses BusyBox 1.20.2, which was released in 2012, and may be vulnerable to other known BusyBox vulnerabilities.	2018-07-24	Aún sin calcular	CVE-2017-3209 MISC CERT-VN BID

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dbus -- dbus	It was found that subscription-manager's DBus interface before 1.19.4 let unprivileged user access the com.redhat.RHSM1.Facts.GetFacts and com.redhat.RHSM1.Config.Set methods. An unprivileged local attacker could use these methods to gain access to private information, or launch a privilege escalation attack.	2018-07-27	Aún sin calcular	CVE-2017-2663 BID CONFIRM CONFIRM
dhc -- dhc_online_shop_app_for_android	The DHC Online Shop App for Android version 3.2.0 and earlier does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.	2018-07-26	Aún sin calcular	CVE-2018-0622 JVN
dotcms -- dotcms	The dotCMS administration panel, versions 3.7.1 and earlier, are vulnerable to cross-site request forgery. The dotCMS administrator panel contains a cross-site request forgery (CSRF) vulnerability. An attacker can perform actions with the same permissions as a victim user, provided the victim has an active session and is induced to trigger the malicious request. An unauthenticated remote attacker may perform actions with the dotCMS administrator panel with the same permissions of a victim user or execute arbitrary system commands with the permissions of the user running the dotCMS application.	2018-07-24	Aún sin calcular	CVE-2017-3187 BID CERT-VN
dotcms -- dotcms	The dotCMS administration panel, versions 3.7.1 and earlier, "Push Publishing" feature in Enterprise Pro is vulnerable to arbitrary file upload. When "Bundle" tar.gz archives uploaded to the Push Publishing feature are decompressed, there are no checks on the types of files which the bundle contains. This vulnerability combined with the path traversal vulnerability (CVE-2017-3188) can lead to remote command execution with the permissions of the user running the dotCMS application. An unauthenticated remote attacker may perform actions with the dotCMS administrator panel with the same permissions of a victim user or execute arbitrary system commands with the permissions of the user running the dotCMS application.	2018-07-24	Aún sin calcular	CVE-2017-3189 BID CERT-VN

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dotcms -- dotcms	The dotCMS administration panel, versions 3.7.1 and earlier, "Push Publishing" feature in Enterprise Pro is vulnerable to path traversal. When "Bundle" tar.gz archives uploaded to the Push Publishing feature are decompressed, the filenames of its contents are not properly checked, allowing for writing files to arbitrary directories on the file system. These archives may be uploaded directly via the administrator panel, or using the CSRF vulnerability (CVE-2017-3187). An unauthenticated remote attacker may perform actions with the dotCMS administrator panel with the same permissions of a victim user or execute arbitrary system commands with the permissions of the user running the dotCMS application.	2018-07-24	Aún sin calcular	CVE-2017-3188 BID CERT-VN
dotnetzip.semvered -- dotnetzip.semvered	DotNetZip.Semvered before 1.11.0 is vulnerable to directory traversal, allowing attackers to write to arbitrary files via a ../ (dot dot slash) in a Zip archive entry that is mishandled during extraction. This vulnerability is also known as 'Zip-Slip'.	2018-07-25	Aún sin calcular	CVE-2018-1002205 CONFIRM CONFIRM MISC MISC MISC
eap -- eap	It was found in EAP 7 before 7.0.9 that properties based files of the management and the application realm configuration that contain user to role mapping are world readable allowing access to users and roles information to all the users logged in to the system.	2018-07-26	Aún sin calcular	CVE-2017-12167 BID REDHAT REDHAT REDHAT REDHAT REDHAT REDHAT REDHAT REDHAT CONFIRM
echelon -- smartserver_and_i.lon	Echelon SmartServer 1 all versions, SmartServer 2 all versions prior to release 4.11.007, i.LON 100 all versions, and i.LON 600 all versions. An attacker can use the SOAP API to retrieve and change sensitive configuration items such as the usernames and passwords for the Web and FTP servers. This vulnerability does not affect the i.LON 600 product.	2018-07-24	Aún sin calcular	CVE-2018-10627 MISC
echelon -- smartserver_and_i.lon	Echelon SmartServer 1 all versions, SmartServer 2 all versions prior to release 4.11.007, i.LON 100 all versions, and i.LON	2018-07-24	Aún sin calcular	CVE-2018-8855 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	600 all versions. The devices allow unencrypted Web connections by default, and devices can receive configuration and firmware updates by unsecure FTP.			
echelon -- smartserver_and_i.lon	Echelon SmartServer 1 all versions, SmartServer 2 all versions prior to release 4.11.007, i.LON 100 all versions, and i.LON 600 all versions. The devices store passwords in plaintext, which may allow an attacker with access to the configuration file to log into the SmartServer web user interface.	2018-07-24	Aún sin calcular	CVE-2018-8851 MISC
echelon -- smartserver_and_i.lon	Echelon SmartServer 1 all versions, SmartServer 2 all versions prior to release 4.11.007, i.LON 100 all versions, and i.LON 600 all versions. An attacker can bypass the required authentication specified in the security configuration file by including extra characters in the directory name when specifying the directory to be accessed. This vulnerability does not affect the i.LON 600 product.	2018-07-24	Aún sin calcular	CVE-2018-8859 MISC
f5 -- big-ip	On F5 BIG-IP DNS 13.1.0-13.1.0.7, 12.1.3-12.1.3.5, DNS Express / DNS Zones accept NOTIFY messages on the management interface from source IP addresses not listed in the 'Allow NOTIFY From' configuration parameter when the db variable "dnsexpress.notifyport" is set to any value other than the default of "0".	2018-07-25	Aún sin calcular	CVE-2018-5538 CONFIRM
f5 -- big-ip	A remote attacker may be able to disrupt services on F5 BIG-IP 13.0.0-13.1.0.5, 12.1.0-12.1.3.5, 11.6.0-11.6.3.1, or 11.2.1-11.5.6 if the TMM virtual server is configured with a HTML or a Rewrite profile. TMM may restart while processing some specially prepared HTML content from the back end.	2018-07-25	Aún sin calcular	CVE-2018-5537 CONFIRM
f5 -- big-ip	A remote attacker via undisclosed measures, may be able to exploit an F5 BIG-IP APM 13.0.0-13.1.0.7 or 12.1.0-12.1.3.5 virtual server configured with an APM per-request policy object and cause a memory leak in the APM module.	2018-07-25	Aún sin calcular	CVE-2018-5536 CONFIRM
f5 -- big-ip	Under certain conditions, on F5 BIG-IP ASM 13.0.0-13.1.0.7, 12.1.0-12.1.3.5, 11.6.0-11.6.3.1, 11.5.1-11.5.6, or 11.2.1, when processing CSRF protections, the BIG-IP ASM	2018-07-25	Aún sin calcular	CVE-2018-5539 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	bd process may restart and produce a core file.			
f5 -- big-ip	Through undisclosed methods, on F5 BIG-IP 13.0.0-13.1.0.7, 12.1.0-12.1.3.5, 11.6.0-11.6.3.1, or 11.2.1-11.5.6, adjacent network attackers can cause a denial of service for VCMP guest and host systems. Attack must be sourced from adjacent network (layer 2).	2018-07-25	Aún sin calcular	CVE-2018-5531 CONFIRM
f5 -- big-ip	When F5 BIG-IP ASM 13.0.0-13.1.0.1, 12.1.0-12.1.3.5, 11.6.0-11.6.3.1, or 11.5.1-11.5.6 is processing HTTP requests, an unusually large number of parameters can cause excessive CPU usage in the BIG-IP ASM bd process.	2018-07-25	Aún sin calcular	CVE-2018-5541 BID CONFIRM
f5 -- big-ip	F5 BIG-IP 13.0.0-13.0.1, 12.1.0-12.1.3.6, or 11.2.1-11.6.3.2 HTTPS health monitors do not validate the identity of the monitored server.	2018-07-25	Aún sin calcular	CVE-2018-5542 CONFIRM
f5 -- big-ip	F5 BIG-IP 13.0.0-13.1.0.5, 12.1.0-12.1.3.5, or 11.6.0-11.6.3.1 virtual servers with HTTP/2 profiles enabled are vulnerable to "HPACK Bomb".	2018-07-25	Aún sin calcular	CVE-2018-5530 CONFIRM
ffmpeg -- ffmpeg	FFmpeg before commit bab0716c7f4793ec42e05a5aa7e80d82a0dd4e75 contains an out of array access vulnerability in MXF format demuxer that can result in DoS. This attack appear to be exploitable via specially crafted MXF file which has to be provided as input. This vulnerability appears to have been fixed in bab0716c7f4793ec42e05a5aa7e80d82a0dd4e75 and later.	2018-07-23	Aún sin calcular	CVE-2018-1999014 BID CONFIRM
ffmpeg -- ffmpeg	FFmpeg before commit 5aba5b89d0b1d73164d3b81764828bb8b20ff32a contains an out of array read vulnerability in ASF_F format demuxer that can result in heap memory reading. This attack appear to be exploitable via specially crafted ASF file that has to provided as input. This vulnerability appears to have been fixed in 5aba5b89d0b1d73164d3b81764828bb8b20ff32a and later.	2018-07-23	Aún sin calcular	CVE-2018-1999015 BID CONFIRM
ffmpeg -- ffmpeg	FFmpeg before commit 9807d3976be0e92e4ece3b4b1701be894cd7c2e1 contains a CWE-835: Infinite loop vulnerability in pva format demuxer that can	2018-07-23	Aún sin calcular	CVE-2018-1999012 BID CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	result in a Vulnerability that allows attackers to consume excessive amount of resources like CPU and RAM. This attack appear to be exploitable via specially crafted PVA file has to be provided as input. This vulnerability appears to have been fixed in 9807d3976be0e92e4ece3b4b1701be894cd7c2e1 and later.			
ffmpeg -- ffmpeg	FFmpeg before commit 2b46ebdbff1d8dec7a3d8ea280a612b91a582869 contains a Buffer Overflow vulnerability in asf_o format demuxer that can result in heap-buffer-overflow that may result in remote code execution. This attack appears to be exploitable via specially crafted ASF file that has to be provided as input to FFmpeg. This vulnerability appears to have been fixed in 2b46ebdbff1d8dec7a3d8ea280a612b91a582869 and later.	2018-07-23	Aún sin calcular	CVE-2018-1999011 BID CONFIRM
ffmpeg -- ffmpeg	FFmpeg before commit a7e032a277452366771951e29fd0bf2bd5c029f0 contains a use-after-free vulnerability in the realmedia demuxer that can result in vulnerability allows attacker to read heap memory. This attack appear to be exploitable via specially crafted RM file has to be provided as input. This vulnerability appears to have been fixed in a7e032a277452366771951e29fd0bf2bd5c029f0 and later.	2018-07-23	Aún sin calcular	CVE-2018-1999013 BID CONFIRM
ffmpeg -- ffmpeg	FFmpeg before commit cced03dd667a5df6df8fd40d8de0bff477ee02e8 contains multiple out of array access vulnerabilities in the mms protocol that can result in attackers accessing out of bound data. This attack appear to be exploitable via network connectivity. This vulnerability appears to have been fixed in cced03dd667a5df6df8fd40d8de0bff477ee02e8 and later.	2018-07-23	Aún sin calcular	CVE-2018-1999010 BID CONFIRM
foreman -- foreman	foreman before version 1.16.0 is vulnerable to a stored XSS in organizations/locations assignment to hosts. Exploiting this requires a user to actively assign hosts to an organization that contains html in its name which is visible to the user prior to taking	2018-07-26	Aún sin calcular	CVE-2017-7535 MLIST BID CONFIRM CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	action.			
fuse -- fuse	In fuse before versions 2.9.8 and 3.x before 3.2.5, fusermount is vulnerable to a restriction bypass when SELinux is active. This allows non-root users to mount a FUSE file system with the 'allow_other' mount option regardless of whether 'user_allow_other' is set in the fuse configuration. An attacker may use this flaw to mount a FUSE file system, accessible by other users, and trick them into accessing files on that file system, possibly causing Denial of Service or other unspecified effects.	2018-07-24	Aún sin calcular	CVE-2018-10906 CONFIRM
gdm -- gdm	A flaw was discovered in gdm 3.24.1 where gdm greeter was no longer setting the ran_once boolean during autologin. If autologin was enabled for a victim, an attacker could simply select 'login as another user' to unlock their screen.	2018-07-26	Aún sin calcular	CVE-2017-12164 CONFIRM CONFIRM
gitlab -- community_and_enterprise_edition	An issue was discovered in GitLab Community and Enterprise Edition before 10.8.7, 11.0.x before 11.0.5, and 11.1.x before 11.1.2. XSS can occur in the branch name during a Web IDE file commit.	2018-07-26	Aún sin calcular	CVE-2018-14605 MISC
gitlab -- community_and_enterprise_edition	An issue was discovered in GitLab Community and Enterprise Edition 11.1.x before 11.1.2. A Denial of Service can occur because Markdown rendering times are slow.	2018-07-26	Aún sin calcular	CVE-2018-14601 MISC
gitlab -- community_and_enterprise_edition	An issue was discovered in GitLab Community and Enterprise Edition before 10.8.7, 11.0.x before 11.0.5, and 11.1.x before 11.1.2. Information Disclosure can occur because the Prometheus metrics feature discloses private project pathnames.	2018-07-26	Aún sin calcular	CVE-2018-14602 MISC
gitlab -- community_and_enterprise_edition	An issue was discovered in GitLab Community and Enterprise Edition before 10.8.7, 11.0.x before 11.0.5, and 11.1.x before 11.1.2. CSRF can occur in the Test feature of the System Hooks component.	2018-07-26	Aún sin calcular	CVE-2018-14603 MISC
gitlab -- community_and_enterprise_edition	An issue was discovered in GitLab Community and Enterprise Edition before 10.8.7, 11.0.x before 11.0.5, and 11.1.x before 11.1.2. XSS can occur via a Milestone name during a promotion.	2018-07-26	Aún sin calcular	CVE-2018-14606 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gitlab -- community_and_enterprise_edition	An issue was discovered in GitLab Community and Enterprise Edition before 10.8.7, 11.0.x before 11.0.5, and 11.1.x before 11.1.2. XSS can occur in the tooltip of the job inside the CI/CD pipeline.	2018-07-26	Aún sin calcular	CVE-2018-14604 MISC
glarysoft -- glary_utilities	Untrusted search path vulnerability in the installer of Glarysoft Glary Utilities (Glary Utilities 5.99 and earlier and Glary Utilities Pro 5.99 and earlier) allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory.	2018-07-26	Aún sin calcular	CVE-2018-0619 JVN
gleez_cms -- gleez_cms	Gleezcms Gleez Cms version 1.3.0 contains a Cross Site Scripting (XSS) vulnerability in Profile page that can result in Inject arbitrary web script or HTML via the profile page editor. This attack appear to be exploitable via The victim must navigate to the attacker's profile page.	2018-07-23	Aún sin calcular	CVE-2018-1999021 CONFIRM
gnome -- gnome	camel/providers/imapx/camel-imapx-server.c in the IMAPx component in GNOME evolution-data-server before 3.21.2 proceeds with cleartext data containing a password if the client wishes to use STARTTLS but the server will not use STARTTLS, which makes it easier for remote attackers to obtain sensitive information by sniffing the network. The server code was intended to report an error and not proceed, but the code was written incorrectly.	2018-07-20	Aún sin calcular	CVE-2016-10727 MISC MISC MISC MISC UBUNTU
gnu -- libredwg	dwg_decode_eed in decode.c in GNU LibreDWG 0.5.1048 leads to a double free (in dwg_free_eed in free.c) because it does not properly manage the obj->eed value after a free occurs.	2018-07-23	Aún sin calcular	CVE-2018-14524 MISC
gnu_mailmain -- mailman	Cross-site scripting vulnerability in Mailman 2.1.26 and earlier allows remote authenticated attackers to inject arbitrary web script or HTML via unspecified vectors.	2018-07-26	Aún sin calcular	CVE-2018-0618 JVN MLIST MLIST DEBIAN
golang -- golang	mholt/archiver golang package before e4ef56d48eb029648b0e895bb0b6a393ef0829c3 is vulnerable to directory traversal, allowing attackers to write to arbitrary files via a ../ (dot dot slash) in an archive entry that is mishandled during extraction. This vulnerability is also known as 'Zip-Slip'.	2018-07-25	Aún sin calcular	CVE-2018-1002207 CONFIRM CONFIRM MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
golemcms -- golemcms	GolemCMS through 2008-12-24, if the install/ directory remains active after an installation, allows remote attackers to execute arbitrary PHP code by inserting this code into the "Database Information" "Table prefix" form field, or obtain sensitive information via a direct request for install/install.sql.	2018-07-24	Aún sin calcular	CVE-2018-14579 MISC
gxlcms -- gxlcms	The add function in www/Lib/Lib/Action/Admin/TplAction.class.php in Gxlcms v1.1.4 allows remote attackers to read arbitrary files via a crafted index.php?s=Admin-Tpl-ADD-id request, related to Lib/Common/Admin/function.php.	2018-07-28	Aún sin calcular	CVE-2018-14685 MISC
h2 -- h2	An issue was discovered in H2 1.4.197. Insecure handling of permissions in the backup function allows attackers to read sensitive files (outside of their permissions) via a symlink to a fake database file.	2018-07-24	Aún sin calcular	CVE-2018-14335 MISC
ibm -- sterling_b2b_integrator_standard_edition	IBM Sterling B2B Integrator Standard Edition (IBM Sterling File Gateway 2.2.0 through 2.2.6) uses weaker than expected cryptographic algorithms that could allow a local attacker to decrypt highly sensitive information. IBM X-Force ID: 132032.	2018-07-20	Aún sin calcular	CVE-2017-1575 CONFIRM BID XF
ibm -- sterling_b2b_integrator_standard_edition	IBM Sterling B2B Integrator Standard Edition 5.2.0 through 5.2.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 141551.	2018-07-23	Aún sin calcular	CVE-2018-1513 CONFIRM XF
ibm -- sterling_b2b_integrator_standard_edition	IBM Sterling B2B Integrator Standard Edition (IBM Sterling File Gateway 2.2.0 through 2.2.6) caches usernames and passwords in browsers that could be used by a local attacker to obtain sensitive information. IBM X-Force ID: 130812.	2018-07-20	Aún sin calcular	CVE-2017-1544 CONFIRM BID XF
ibm -- sterling_file_gateway	IBM Sterling File Gateway 2.2.0 through 2.2.6 could allow a remote authenticated attacker to obtain sensitive information displayed in the URL that could lead to further attacks against the system. IBM X-Force ID: 140688.	2018-07-20	Aún sin calcular	CVE-2018-1470 CONFIRM BID XF

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- websphere_mq	IBM WebSphere MQ 7.5, 8.0, and 9.0 could allow a remotely authenticated attacker to to send invalid or malformed headers that could cause messages to no longer be transmitted via the affected channel. IBM X-Force ID: 141339.	2018-07-23	Aún sin calcular	CVE-2018-1503 CONFIRM SECTRACK XF
idreamsoft -- icms	An SSRF vulnerability was discovered in idreamsoft iCMS V7.0.9 that allows attackers to read sensitive files, access an intranet, or possibly have unspecified other impact.	2018-07-23	Aún sin calcular	CVE-2018-14514 MISC
imagemagick -- imagemagick	The ReadMATImageV4 function in coders/mat.c in ImageMagick 7.0.8-7 uses an uninitialized variable, leading to memory corruption.	2018-07-23	Aún sin calcular	CVE-2018-14551 MISC
ipa -- ipa	A vulnerability was found in ipa before 4.4. IdM's ca-del, ca-disable, and ca-enable commands did not properly check the user's permissions while modifying CAs in Dogtag. An authenticated, unauthorized attacker could use this flaw to delete, disable, or enable CAs causing various denial of service problems with certificate issuance, OCSP signing, and deletion of secret keys.	2018-07-27	Aún sin calcular	CVE-2017-2590 REDHAT BID CONFIRM
jbpmmigration -- jbpmmigration	It was discovered that the XmlUtils class in jbpmmigration 6.5 performed expansion of external parameter entities while parsing XML files. A remote attacker could use this flaw to read files accessible to the user running the application server and, potentially, perform other more advanced XML eXternal Entity (XXE) attacks.	2018-07-26	Aún sin calcular	CVE-2017-7545 BID REDHAT REDHAT CONFIRM CONFIRM
jenkins -- jenkins	A cross-site scripting vulnerability exists in Jenkins 2.132 and earlier, 2.121.1 and earlier in the Stapler web framework's org/kohsuke/stapler/Stapler.java that allows attackers with the ability to control the existence of some URLs in Jenkins to define JavaScript that would be executed in another user's browser when that other user views HTTP 404 error pages while Stapler debug mode is enabled.	2018-07-23	Aún sin calcular	CVE-2018-1999007 CONFIRM
jenkins -- jenkins	It was found that the use of Pipeline: Classpath Step Jenkins plugin enables a bypass of the Script Security sandbox for users with SCM commit access, as well as users with e.g. Job/Configure permission in Jenkins.	2018-07-27	Aún sin calcular	CVE-2017-2650 BID CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jenkins -- jenkins	It was found that there were no permission checks performed in the Distributed Fork plugin before and including 1.5.0 for Jenkins that provides the dist-fork CLI command beyond the basic check for Overall/Read permission, allowing anyone with that permission to run arbitrary shell commands on all connected nodes.	2018-07-27	Aún sin calcular	CVE-2017-2652 BID CONFIRM
jenkins -- jenkins	A exposure of sensitive information vulnerability exists in Jenkins 2.132 and earlier, 2.121.1 and earlier in Plugin.java that allows attackers to determine the date and time when a plugin HPI/JPI file was last extracted, which typically is the date of the most recent installation/upgrade.	2018-07-23	Aún sin calcular	CVE-2018-1999006 CONFIRM
jenkins -- jenkins	It was found that jenkins-ssh-slaves-plugin before version 1.15 did not perform host key verification, thereby enabling Man-in-the-Middle attacks.	2018-07-27	Aún sin calcular	CVE-2017-2648 BID CONFIRM CONFIRM
jenkins -- jenkins	A Improper authorization vulnerability exists in Jenkins 2.132 and earlier, 2.121.1 and earlier in Queue.java that allows attackers with Overall/Read permission to cancel queued builds.	2018-07-23	Aún sin calcular	CVE-2018-1999003 CONFIRM
jenkins -- jenkins	A arbitrary file read vulnerability exists in Jenkins 2.132 and earlier, 2.121.1 and earlier in the Stapler web framework's org/kohsuke/stapler/Stapler.java that allows attackers to send crafted HTTP requests returning the contents of any file on the Jenkins master file system that the Jenkins master has access to.	2018-07-23	Aún sin calcular	CVE-2018-1999002 CONFIRM
jenkins -- jenkins	jenkins-mailer-plugin before version 1.20 is vulnerable to an information disclosure while using the feature to send emails to a dynamically created list of users based on the changelogs. This could in some cases result in emails being sent to people who have no user account in Jenkins, and in rare cases even people who were not involved in whatever project was being built, due to some mapping based on the local-part of email addresses.	2018-07-27	Aún sin calcular	CVE-2017-2651 BID CONFIRM CONFIRM
jenkins -- jenkins	It was found that the Active Directory Plugin for Jenkins up to and including version 2.2 did not verify certificates of the Active Directory server, thereby enabling Man-in-	2018-07-27	Aún sin calcular	CVE-2017-2649 BID CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the-Middle attacks.			
jenkins -- jenkins	A unauthorized modification of configuration vulnerability exists in Jenkins 2.132 and earlier, 2.121.1 and earlier in User.java that allows attackers to provide crafted login credentials that cause Jenkins to move the config.xml file from the Jenkins home directory. If Jenkins is started without this file present, it will revert to the legacy defaults of granting administrator access to anonymous users.	2018-07-23	Aún sin calcular	CVE-2018-1999001 CONFIRM
jenkins -- jenkins	A cross-site scripting vulnerability exists in Jenkins 2.132 and earlier, 2.121.1 and earlier in BuildTimelineWidget.java, BuildTimelineWidget/control.jelly that allows attackers with Job/Configure permission to define JavaScript that would be executed in another user's browser when that other user performs some UI actions.	2018-07-23	Aún sin calcular	CVE-2018-1999005 CONFIRM
jenkins -- jenkins	A Improper authorization vulnerability exists in Jenkins 2.132 and earlier, 2.121.1 and earlier in SlaveComputer.java that allows attackers with Overall/Read permission to initiate agent launches, and abort in-progress agent launches.	2018-07-23	Aún sin calcular	CVE-2018-1999004 CONFIRM
joyplus-cms -- joyplus-cms	joyplus-cms 1.6.0 has XSS via the manager/collect/collect_vod_zhuiju.php keyword parameter.	2018-07-22	Aún sin calcular	CVE-2018-14500 MISC
joyplus-cms -- joyplus-cms	manager/admin_ajax.php in joyplus-cms 1.6.0 has SQL Injection, as demonstrated by crafted POST data beginning with an "m_id=1 AND SLEEP(5)" substring.	2018-07-22	Aún sin calcular	CVE-2018-14501 MISC
katello-debug -- katello-debug	A flaw was found in katello-debug before 3.4.0 where certain scripts and log files used insecure temporary files. A local user could exploit this flaw to conduct a symbolic-link attack, allowing them to overwrite the contents of arbitrary files.	2018-07-27	Aún sin calcular	CVE-2016-9595 REDHAT CONFIRM
keycloak -- keycloak	It was found that while parsing the SAML messages the StaxParserUtil class of keycloak before 2.5.1 replaces special strings for obtaining attribute values with system property. This could allow an attacker to determine values of system properties at the attacked system by formatting the SAML request ID field to be the chosen system	2018-07-26	Aún sin calcular	CVE-2017-2582 BID REDHAT REDHAT REDHAT REDHAT REDHAT REDHAT

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	property which could be obtained in the "InResponseTo" field in the response.			REDHAT REDHAT REDHAT CONFIRM CONFIRM
keycloak -- keycloak	keycloak before version 4.0.0.final is vulnerable to a infinite loop in session replacement. A Keycloak cluster with multiple nodes could mishandle an expired session replacement and lead to an infinite loop. A malicious authenticated user could use this flaw to achieve Denial of Service on the server.	2018-07-23	Aún sin calcular	CVE-2018-10912 CONFIRM
keycloak -- keycloak	It was found that when Keycloak before 2.5.5 receives a Logout request with a Extensions in the middle of the request, the SAMLSloRequestParser.parse() method ends in a infinite loop. An attacker could use this flaw to conduct denial of service attacks.	2018-07-27	Aún sin calcular	CVE-2017-2646 BID CONFIRM
krb5 -- krb5	An authentication bypass flaw was found in the way krb5's certauth interface before 1.16.1 handled the validation of client certificates. A remote attacker able to communicate with the KDC could potentially use this flaw to impersonate arbitrary principals under rare and erroneous circumstances.	2018-07-26	Aún sin calcular	CVE-2017-7562 BID REDHAT CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM
lenovo -- multiple_products	The IMM2 First Failure Data Capture function collects management module logs and diagnostic information when a hardware error is detected. This information is made available for download through an SFTP server hosted on the IMM2 management network interface. In versions earlier than 4.90 for Lenovo System x and earlier than 6.80 for IBM System x, the credentials to access the SFTP server are hard-coded and described in the IMM2 documentation, allowing an attacker with management network access to obtain the collected FFDC data. After applying the update, the IMM2 will create random SFTP credentials for use with OneCLI.	2018-07-26	Aún sin calcular	CVE-2018-9068 CONFIRM
libgcrypt -- libgcrypt	libgcrypt before version 1.7.8 is vulnerable to a cache side-channel attack resulting into a complete break of RSA-1024 while using the left-to-right method for computing the	2018-07-26	Aún sin calcular	CVE-2017-7526 BID SECTRACK CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	sliding-window expansion. The same attack is believed to work on RSA-2048 with moderately more computation. This side-channel requires that attacker can run arbitrary software on the hardware where the private RSA key is used.			MISC CONFIRM CONFIRM CONFIRM MLIST DEBIAN DEBIAN
libice -- libice	It was discovered that libICE before 1.0.9-8 used a weak entropy to generate keys. A local attacker could potentially use this flaw for session hijacking using the information available from the process list.	2018-07-27	Aún sin calcular	CVE-2017-2626 BID SECTRACK REDHAT CONFIRM CONFIRM GENTOO MISC
liblouis -- liblouis	A missing patch for a stack-based buffer overflow in findTable() was found in Red Hat version of liblouis before 2.5.4. An attacker could cause a denial of service condition or potentially even arbitrary code execution.	2018-07-27	Aún sin calcular	CVE-2017-15101 REDHAT CONFIRM
libmspack -- libmspack	An issue was discovered in mspack/chmd.c in libmspack before 0.7alpha. There is an off-by-one error in the TOLOWER() macro for CHM decompression.	2018-07-28	Aún sin calcular	CVE-2018-14682 MISC MISC MISC
libmspack -- libmspack	An issue was discovered in kwajd_read_headers in mspack/kwajd.c in libmspack before 0.7alpha. Bad KWAJ file header extensions could cause a one or two byte overwrite.	2018-07-28	Aún sin calcular	CVE-2018-14681 MISC MISC MISC
libmspack -- libmspack	An issue was discovered in mspack/chmd.c in libmspack before 0.7alpha. There is an off-by-one error in the CHM PMGI/PMGL chunk number validity checks, which could lead to denial of service (uninitialized data dereference and application crash).	2018-07-28	Aún sin calcular	CVE-2018-14679 MISC MISC MISC
libmspack -- libmspack	An issue was discovered in mspack/chmd.c in libmspack before 0.7alpha. It does not reject blank CHM filenames.	2018-07-28	Aún sin calcular	CVE-2018-14680 MISC MISC MISC
libwav -- libwav	An issue has been found in libwav through 2017-04-20. It is a SEGV in the function wav_write in libwav.c.	2018-07-23	Aún sin calcular	CVE-2018-14549 MISC MISC
libxdmcp -- libxdmcp	It was discovered that libXdmcp before 1.1.2 including used weak entropy to generate session keys. On a multi-user system using xdmcp, a local attacker could potentially use	2018-07-27	Aún sin calcular	CVE-2017-2625 BID SECTRACK REDHAT

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	information available from the process list to brute force the key, allowing them to hijack other users' sessions.			CONFIRM GENTOO MISC
lica -- minicmts_e8k_devices	LICA miniCMTS E8K(u/i/...) devices allow remote attackers to obtain sensitive information via a direct POST request for the inc/user.ini file, leading to discovery of a password hash.	2018-07-25	Aún sin calcular	CVE-2018-14083 MISC
linux -- linux_kernel	An issue was discovered in the Linux kernel through 4.17.10. There is a buffer overflow in truncate_inline_inode() in fs/f2fs/inline.c when umounting an f2fs image, because a length value may be negative.	2018-07-27	Aún sin calcular	CVE-2018-14615 MISC
linux -- linux_kernel	An issue was discovered in the Linux kernel through 4.17.10. There is an out-of-bounds access in __remove_dirty_segment() in fs/f2fs/segment.c when mounting an f2fs image.	2018-07-27	Aún sin calcular	CVE-2018-14614 MISC
linux -- linux_kernel	A flaw was found in Linux kernel's KVM virtualization subsystem. The VMX code does not restore the GDT.LIMIT to the previous host value, but instead sets it to 64KB. With a corrupted GDT limit a host's userspace code has an ability to place malicious entries in the GDT, particularly to the per-cpu variables. An attacker can use this to escalate their privileges.	2018-07-26	Aún sin calcular	CVE-2018-10901 CONFIRM CONFIRM
linux -- linux_kernel	Linux kernel is vulnerable to a stack-out-of-bounds write in the ext4 filesystem code when mounting and writing to a crafted ext4 image in ext4_update_inline_data(). An attacker could use this to cause a system crash and a denial of service.	2018-07-25	Aún sin calcular	CVE-2018-10880 CONFIRM CONFIRM CONFIRM CONFIRM MLIST
linux -- linux_kernel	An issue was discovered in the Linux kernel through 4.17.10. There is a NULL pointer dereference and panic in hfsplus_lookup() in fs/hfsplus/dir.c when opening a file (that is purportedly a hard link) in an hfs+ filesystem that has malformed catalog data, and is mounted read-only without a metadata directory.	2018-07-27	Aún sin calcular	CVE-2018-14617 MISC MISC
linux -- linux_kernel	It was found that the Linux kernel's Datagram Congestion Control Protocol (DCCP) implementation before 2.6.22.17 used the IPv4-only inet_sk_rebuild_header() function for both IPv4 and IPv6 DCCP	2018-07-27	Aún sin calcular	CVE-2017-2634 REDHAT REDHAT REDHAT BID

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	connections, which could result in memory corruptions. A remote attacker could use this flaw to crash the system.			SECTRACK CONFIRM CONFIRM
linux -- linux_kernel	An issue was discovered in the Linux kernel through 4.17.10. There is out-of-bounds access in write_extent_buffer() when mounting and operating a crafted btrfs image, because of a lack of verification that each block group has a corresponding chunk at mount time, within btrfs_read_block_groups in fs/btrfs/extent-tree.c.	2018-07-27	Aún sin calcular	CVE-2018-14610 MISC MISC
linux -- linux_kernel	A flaw was found in the Linux kernel's handling of clearing SELinux attributes on /proc/pid/attr files before 4.9.10. An empty (null) write to this file can crash the system by causing the system to attempt to access unmapped kernel memory.	2018-07-27	Aún sin calcular	CVE-2017-2618 BID REDHAT REDHAT REDHAT CONFIRM CONFIRM MLIST DEBIAN
linux -- linux_kernel	An issue was discovered in the Linux kernel through 4.17.11, as used in Xen through 4.11.x. The xen_failsafe_callback entry point in arch/x86/entry/entry_64.S does not properly maintain RBX, which allows local users to cause a denial of service (uninitialized memory usage and system crash). Within Xen, 64-bit x86 PV Linux guest OS users can trigger a guest OS crash or possibly gain privileges.	2018-07-28	Aún sin calcular	CVE-2018-14678 MISC
linux -- linux_kernel	A kernel data leak due to an out-of-bound read was found in the Linux kernel in inet_diag_msg_sctp{,l}addr_fill() and sctp_get_sctp_info() functions present since version 4.7-rc1 through version 4.13. A data leak happens when these functions fill in sockaddr data structures used to export socket's diagnostic information. As a result, up to 100 bytes of the slab data could be leaked to a userspace.	2018-07-26	Aún sin calcular	CVE-2017-7558 MLIST BID SECTRACK REDHAT REDHAT REDHAT CONFIRM MLIST DEBIAN
linux -- linux_kernel	A flaw was found in the Linux kernel's ext4 filesystem. A local user can cause an out-of-bounds write and a denial of service or unspecified other impact is possible by mounting and operating a crafted ext4 filesystem image.	2018-07-26	Aún sin calcular	CVE-2018-10878 CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				CONFIRM MLIST
linux -- linux_kernel	An issue was discovered in the Linux kernel through 4.17.10. There is an invalid pointer dereference in io_ctl_map_page() when mounting and operating a crafted btrfs image, because of a lack of block group item validation in check_leaf_item in fs/btrfs/tree-checker.c.	2018-07-27	Aún sin calcular	CVE-2018-14613 MISC MISC
linux -- linux_kernel	An issue was discovered in the Linux kernel through 4.17.10. There is an invalid pointer dereference in __del_reloc_root() in fs/btrfs/relocation.c when mounting a crafted btrfs image, related to removing reloc rb_trees when reloc control has not been initialized.	2018-07-27	Aún sin calcular	CVE-2018-14609 MISC MISC
linux -- linux_kernel	An issue was discovered in the Linux kernel through 4.17.10. There is an invalid pointer dereference in btrfs_root_node() when mounting a crafted btrfs image, because of a lack of chunk block group mapping validation in btrfs_read_block_groups in fs/btrfs/extent-tree.c, and a lack of empty-tree checks in check_leaf in fs/btrfs/tree-checker.c.	2018-07-27	Aún sin calcular	CVE-2018-14612 MISC MISC MISC
linux -- linux_kernel	A flaw was found in the Linux kernel's ext4 filesystem. A local user can cause an out-of-bound access in ext4_get_group_info function, a denial of service, and a system crash by mounting and operating on a crafted ext4 filesystem image.	2018-07-26	Aún sin calcular	CVE-2018-10881 CONFIRM CONFIRM CONFIRM CONFIRM MLIST
linux -- linux_kernel	A flaw was found in the Linux kernel's ext4 filesystem. A local user can cause a use-after-free in ext4_xattr_set_entry function and a denial of service or unspecified other impact may occur by renaming a file in a crafted ext4 filesystem image.	2018-07-26	Aún sin calcular	CVE-2018-10879 CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM MLIST
linux -- linux_kernel	A flaw was found in Linux kernel in the ext4 filesystem code. A use-after-free is possible in ext4_ext_remove_space() function when mounting and operating a crafted ext4 image.	2018-07-26	Aún sin calcular	CVE-2018-10876 CONFIRM CONFIRM CONFIRM CONFIRM MLIST
linux --	A flaw was found in the Linux kernel's ext4	2018-07-27	Aún sin calcular	CVE-2018-10882

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
linux_kernel	filesystem. A local user can cause an out-of-bound write in in fs/jbd2/transaction.c code, a denial of service, and a system crash by unmounting a crafted ext4 filesystem image.			CONFIRM CONFIRM CONFIRM MLIST
linux -- linux_kernel	An issue was discovered in the Linux kernel through 4.17.10. There is a use-after-free in try_merge_free_space() when mounting a crafted btrfs image, because of a lack of chunk type flag checks in btrfs_check_chunk_valid in fs/btrfs/volumes.c.	2018-07-27	Aún sin calcular	CVE-2018-14611 MISC MISC
linux -- linux_kernel	The timer_create syscall implementation in kernel/time/posix-timers.c in the Linux kernel before 4.14.8 doesn't properly validate the sigevent->sigev_notify field, which leads to out-of-bounds access in the show_timer function (called when /proc/$PID/timers is read). This allows userspace applications to read arbitrary kernel memory (on a kernel built with CONFIG_POSIX_TIMERS and CONFIG_CHECKPOINT_RESTORE).	2018-07-26	Aún sin calcular	CVE-2017-18344 MISC MISC
linux -- linux_kernel	An issue was discovered in the Linux kernel through 4.17.10. There is a NULL pointer dereference in fscrypt_do_page_crypto() in fs/crypto/crypto.c when operating on a file in a corrupted f2fs image.	2018-07-27	Aún sin calcular	CVE-2018-14616 MISC
linux -- util-linux	A race condition was found in util-linux before 2.32.1 in the way su handled the management of child processes. A local authenticated attacker could use this flaw to kill other processes with root privileges under specific conditions.	2018-07-27	Aún sin calcular	CVE-2017-2616 REDHAT BID SECTRACK REDHAT CONFIRM CONFIRM GENTOO DEBIAN
logicool -- connection_utility_software	Untrusted search path vulnerability in LOGICOOL CONNECTION UTILITY SOFTWARE versions before 2.30.9 allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory.	2018-07-26	Aún sin calcular	CVE-2018-0621 JVN
logicool -- game_software	Untrusted search path vulnerability in LOGICOOL Game Software versions before 8.87.116 allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory.	2018-07-26	Aún sin calcular	CVE-2018-0620 JVN

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mathjax -- mathjax	MathJax version prior to version 2.7.4 contains a Cross Site Scripting (XSS) vulnerability in the \unicode{} macro that can result in Potentially untrusted Javascript running within a web browser. This attack appear to be exploitable via The victim must view a page where untrusted content is processed using Mathjax. This vulnerability appears to have been fixed in 2.7.4 and later.	2018-07-23	Aún sin calcular	CVE-2018-1999024 MISC CONFIRM
mcafee -- data_loss_prevention	Exploiting Incorrectly Configured Access Control Security Levels vulnerability in McAfee Data Loss Prevention (DLP) for Windows versions prior to 10.0.505 and 11.0.405 allows local users to bypass DLP policy via editing of local policy files when offline.	2018-07-23	Aún sin calcular	CVE-2018-6683 CONFIRM
mcafee -- drive_encryption	Authentication Bypass vulnerability in TPM autoboot in McAfee Drive Encryption (MDE) 7.1.0 and above allows physically proximate attackers to bypass local security protection via specific set of circumstances.	2018-07-27	Aún sin calcular	CVE-2018-6686 CONFIRM
mcafee -- web_gateway	Configuration/Environment manipulation vulnerability in the administrative interface in McAfee Web Gateway (MWG) MWG 7.8.1.x allows authenticated administrator users to execute arbitrary commands via unspecified vectors.	2018-07-23	Aún sin calcular	CVE-2018-6678 BID CONFIRM
mcafee -- web_gateway	Directory Traversal vulnerability in the administrative user interface in McAfee Web Gateway (MWG) MWG 7.8.1.x allows authenticated administrator users to gain elevated privileges via unspecified vectors.	2018-07-23	Aún sin calcular	CVE-2018-6677 BID CONFIRM
mitmproxy -- mitmproxy	mitmweb in mitmproxy v4.0.3 allows DNS Rebinding attacks, related to tools/web/app.py.	2018-07-22	Aún sin calcular	CVE-2018-14505 CONFIRM CONFIRM
moxa -- nport	In Moxa NPort 5210, 5230, and 5232 versions 2.9 build 17030709 and prior, the amount of resources requested by a malicious actor are not restricted, allowing for a denial-of-service condition.	2018-07-24	Aún sin calcular	CVE-2018-10632 BID MISC
multiple_vendors -- das_u-boot_aes-cbc_encryption	Das U-Boot is a device bootloader that can read its configuration from an AES encrypted file. For devices utilizing this environment encryption mode, U-Boot's use of a zero initialization vector may allow attacks	2018-07-24	Aún sin calcular	CVE-2017-3225 BID CERT-VN

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	against the underlying cryptographic implementation and allow an attacker to decrypt the data. Das U-Boot's AES-CBC encryption feature uses a zero (0) initialization vector. This allows an attacker to perform dictionary attacks on encrypted data produced by Das U-Boot to learn information about the encrypted data.			
multiple_vendors -- das_u-boot_aes-cbc_encryption	Das U-Boot is a device bootloader that can read its configuration from an AES encrypted file. Devices that make use of Das U-Boot's AES-CBC encryption feature using environment encryption (i.e., setting the configuration parameter CONFIG_ENV_AES=y) read environment variables from disk as the encrypted disk image is processed. An attacker with physical access to the device can manipulate the encrypted environment data to include a crafted two-byte sequence which triggers an error in environment variable parsing. This error condition is improperly handled by Das U-Boot, resulting in an immediate process termination with a debugging message.	2018-07-24	Aún sin calcular	CVE-2017-3226 BID CERT-VN
multiple_vendors -- multiple_products	Applications developed using the Portrait Display SDK, versions 2.30 through 2.34, default to insecure configurations which allow arbitrary code execution. A number of applications developed using the Portrait Displays SDK do not use secure permissions when running. These applications run the component pdiservice.exe with NT AUTHORITY/SYSTEM permissions. This component is also read/writable by all Authenticated Users. This allows local authenticated attackers to run arbitrary code with SYSTEM privileges. The following applications have been identified by Portrait Displays as affected: Fujitsu DisplayView Click: Version 6.0 and 6.01. The issue was fixed in Version 6.3. Fujitsu DisplayView Click Suite: Version 5. The issue is addressed by patch in Version 5.9. HP Display Assistant: Version 2.1. The issue was fixed in Version 2.11. HP My Display: Version 2.0. The issue was fixed in Version 2.1. Philips Smart Control Premium: Versions 2.23, 2.25. The issue was fixed in Version 2.26.	2018-07-24	Aún sin calcular	CVE-2017-3210 CERT-VN BID

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
multiple_vendors -- open_shortest_path_first_protocol	Open Shortest Path First (OSPF) protocol implementations may improperly determine Link State Advertisement (LSA) recency for LSAs with MaxSequenceNumber. According to RFC 2328 section 13.1, for two instances of the same LSA, recency is determined by first comparing sequence numbers, then checksums, and finally MaxAge. In a case where the sequence numbers are the same, the LSA with the larger checksum is considered more recent, and will not be flushed from the Link State Database (LSDB). Since the RFC does not explicitly state that the values of links carried by a LSA must be the same when prematurely aging a self-originating LSA with MaxSequenceNumber, it is possible in vulnerable OSPF implementations for an attacker to craft a LSA with MaxSequenceNumber and invalid links that will result in a larger checksum and thus a 'newer' LSA that will not be flushed from the LSDB. Propagation of the crafted LSA can result in the erasure or alteration of the routing tables of routers within the routing domain, creating a denial of service condition or the re-routing of traffic on the network. CVE-2017-3224 has been reserved for Quagga and downstream implementations (SUSE, openSUSE, and Red Hat packages).	2018-07-24	Aún sin calcular	CVE-2017-3224 CERT-VN
navarino -- infinity_web_interface	Navarino Infinity web interface up to version 2.2 exposes an unauthenticated script that is prone to blind sql injection. If successfully exploited the user can get info from the underlying postgresql database that could lead into to total compromise of the product. The said script is available with no authentication.	2018-07-24	Aún sin calcular	CVE-2018-5384 BID MISC MISC CERT-VN
navarino -- infinity_web_interface	Some Navarino Infinity functions, up to version 2.2, placed in the URL can bypass any authentication mechanism leading to an information leak.	2018-07-24	Aún sin calcular	CVE-2018-5386 BID MISC MISC CERT-VN
navarino -- infinity_web_interface	Navarino Infinity is prone to session fixation attacks. The server accepts the session ID as a GET parameter which can lead to bypassing the two factor authentication in some installations. This could lead to	2018-07-24	Aún sin calcular	CVE-2018-5385 BID MISC MISC CERT-VN

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	phishing attacks that can bypass the two factor authentication that is present in some installations.			
nec_platforms -- csdx_and_csdj_series_products	NEC Platforms Calsos CSDX and CSDJ series products (CSDX 1.37210411 and earlier, CSDX(P) 4.37210411 and earlier, CSDX(D) 3.37210411 and earlier, CSDX(S) 2.37210411 and earlier, CSDJ-B 01.03.00 and earlier, CSDJ-H 01.03.00 and earlier, CSDJ-D 01.03.00 and earlier, CSDJ-A 03.00.00) allows remote authenticated attackers to bypass access restriction to conduct arbitrary operations with administrative privilege via unspecified vectors.	2018-07-26	Aún sin calcular	CVE-2018-0613 JVN CONFIRM
nec_platforms -- csdx_and_csdj_series_products	Cross-site scripting vulnerability in NEC Platforms Calsos CSDX and CSDJ series products (CSDX 1.37210411 and earlier, CSDX(P) 4.37210411 and earlier, CSDX(D) 3.37210411 and earlier, CSDX(S) 2.37210411 and earlier, CSDJ-B 01.03.00 and earlier, CSDJ-H 01.03.00 and earlier, CSDJ-D 01.03.00 and earlier, CSDJ-A 03.00.00) allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2018-07-26	Aún sin calcular	CVE-2018-0614 JVN CONFIRM
netgear -- dgn2200_router	A vulnerability is in the 'BSW_cxttongr.htm' page of the Netgear DGN2200, version DGN2200-V1.0.0.50_7.0.50, and DGND3700, version DGND3700-V1.0.0.17_1.0.17, which can allow a remote attacker to access this page without any authentication. When processed, it exposes the admin password in clear text before it gets redirected to absw_vfysucc.cgia. An attacker can use this password to gain administrator access to the targeted router's web interface.	2018-07-24	Aún sin calcular	CVE-2016-5649 MISC
netgear -- wndr4500_router	There are few web pages associated with the genie app on the Netgear WNDR4500 running firmware version V1.0.1.40_1.0.6877. Genie app adds some capabilities over the Web GUI and can be accessed even when you are away from home. A remote attacker can access genie_ping.htm or genie_ping2.htm or genie_ping3.htm page without authentication. Once accessed, the page will be redirected to the aCongratulations2.htma page, which reveals some sensitive	2018-07-24	Aún sin calcular	CVE-2016-5638 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	information such as 2.4GHz & 5GHz Wireless Network Name (SSID) and Network Key (Password) in clear text.			
netpbm -- netpbm	An out-of-bounds write vulnerability was found in netpbm before 10.61. A maliciously crafted file could cause the application to crash or possibly allow code execution.	2018-07-27	Aún sin calcular	CVE-2017-2580 BID CONFIRM
netpbm -- netpbm	An out-of-bounds read vulnerability was found in netpbm before 10.61. The expandCodeOntoStack() function has an insufficient code value check, so that a maliciously crafted file could cause the application to crash or possibly allows code execution.	2018-07-27	Aún sin calcular	CVE-2017-2579 BID CONFIRM
netpbm -- netpbm	A null pointer dereference vulnerability was found in netpbm before 10.61. A maliciously crafted SVG file could cause the application to crash.	2018-07-27	Aún sin calcular	CVE-2017-2586 BID CONFIRM
netpbm -- netpbm	A memory allocation vulnerability was found in netpbm before 10.61. A maliciously crafted SVG file could cause the application to crash.	2018-07-27	Aún sin calcular	CVE-2017-2587 BID CONFIRM
netpbm -- netpbm	An out-of-bounds write vulnerability was found in netpbm before 10.61. A maliciously crafted file could cause the application to crash or possibly allow code execution.	2018-07-27	Aún sin calcular	CVE-2017-2581 BID CONFIRM
network -- manager_vpnc	Network Manager VPNC plugin (aka networkmanager-vpnc) before version 1.2.6 is vulnerable to a privilege escalation attack. A new line character can be used to inject a Password helper parameter into the configuration data passed to VPNC, allowing an attacker to execute arbitrary commands as root.	2018-07-26	Aún sin calcular	CVE-2018-10900 CONFIRM CONFIRM CONFIRM CONFIRM MISC DEBIAN
niushop -- b2b2c_multi-business_basic	A file upload vulnerability in application/shop/controller/member.php in Niushop B2B2C Multi-business basic version V1.11 allows any remote member to upload a .php file to the web server via a profile avatar field, by using an image Content-Type (e.g., image/jpeg) with a modified filename and file content. This results in arbitrary code execution by requesting that .php file.	2018-07-23	Aún sin calcular	CVE-2018-14570 MISC
october -- cms	October CMS version prior to build 437 contains a Cross Site Scripting (XSS) vulnerability in the Media module and	2018-07-23	Aún sin calcular	CVE-2018-1999008 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	create folder functionality that can result in an Authenticated user with media module permission creating arbitrary folder name with XSS content. This attack appear to be exploitable via an Authenticated user with media module permission who can create arbitrary folder name (XSS). This vulnerability appears to have been fixed in build 437.			
october -- cms	October CMS version prior to Build 437 contains a Local File Inclusion vulnerability in modules/system/traits/ViewMaker.php#244 (makeFileContents function) that can result in Sensitive information disclosure and remote code execution. This attack appear to be exploitable remotely if the /backend path is accessible. This vulnerability appears to have been fixed in Build 437.	2018-07-23	Aún sin calcular	CVE-2018-1999009 CONFIRM
open-audit -- community	Cross-site scripting (XSS) vulnerability in the Groups Page in Open-Audit Community 2.2.6 allows remote attackers to inject arbitrary web script or HTML via the group name.	2018-07-25	Aún sin calcular	CVE-2018-14493 MISC
open_networking_foundation -- onos	Open Networking Foundation (ONF) ONOS version 1.13.2 and earlier version contains a Directory Traversal vulnerability in core/common/src/main/java/org/onosproject/common/app/ApplicationArchive.java line 35 that can result in arbitrary file deletion (overwrite). This attack appear to be exploitable via a specially crafted zip file should be uploaded.	2018-07-23	Aún sin calcular	CVE-2018-1999020 MISC CONFIRM
openshift -- enterprise	A flaw was found in all Openshift Enterprise versions using the openshift elasticsearch plugin. An attacker with knowledge of the given name used to authenticate and access Elasticsearch can later access it without the token, bypassing authentication. This attack also requires that the Elasticsearch be configured with an external route, and the data accessed is limited to the indices.	2018-07-27	Aún sin calcular	CVE-2017-12195 REDHAT REDHAT CONFIRM
ovirt-engine -- ovirt-engine	ovirt-engine before version 4.1.7.6 with log level set to DEBUG includes passwords in the log file without masking. Only administrators can change the log level and only administrators can access the logs. This presents a risk when debug-level logs are shared with vendors or other parties to	2018-07-27	Aún sin calcular	CVE-2017-15113 BID REDHAT CONFIRM CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	troubleshoot issues.			
pear -- html_quickform	PEAR HTML_QuickForm version 3.2.14 contains an eval injection (CWE-95) vulnerability in HTML_QuickForm's getSubmitValue method, HTML_QuickForm's validate method, HTML_QuickForm_hierselect's _setOptions method, HTML_QuickForm_element's _findValue method, HTML_QuickForm_element's _prepareValue method. that can result in Possible information disclosure, possible impact on data integrity and execution of arbitrary code. This attack appear to be exploitable via A specially crafted query string could be utilised, e.g. http://www.example.com/admin/add_practice_type_id[1]=fubar%27])%20OR%20die(%27OOK!%27);%20//&mode=live. This vulnerability appears to have been fixed in 3.2.15.	2018-07-23	Aún sin calcular	CVE-2018-1999022 CONFIRM CONFIRM
pidgin -- pidgin	An out-of-bounds write flaw was found in the way Pidgin before 2.12.0 processed XML content. A malicious remote server could potentially use this flaw to crash Pidgin or execute arbitrary code in the context of the pidgin process.	2018-07-27	Aún sin calcular	CVE-2017-2640 BID REDHAT CONFIRM GENTOO DEBIAN
pivotal -- application_service	Pivotal Apps Manager included in Pivotal Application Service, versions 2.2.x prior to 2.2.1 and 2.1.x prior to 2.1.8 and 2.0.x prior to 2.0.17 and 1.12.x prior to 1.12.26, does not escape all user-provided content when sending invitation emails. A malicious authenticated user can inject content into an invite to another user, exploiting the trust implied by the source of the email.	2018-07-24	Aún sin calcular	CVE-2018-11044 CONFIRM
plexus-archiver -- plexus-archiver	plexus-archiver before 3.6.0 is vulnerable to directory traversal, allowing attackers to write to arbitrary files via a ../ (dot dot slash) in an archive entry that is mishandled during extraction. This vulnerability is also known as 'Zip-Slip'.	2018-07-25	Aún sin calcular	CVE-2018-1002200 REDHAT REDHAT CONFIRM CONFIRM MISC MISC MISC DEBIAN
poppler -- poppler	Poppler through 0.62 contains a Buffer Overflow vulnerability due to an incorrect	2018-07-25	Aún sin calcular	CVE-2018-13988 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	memory access that is not mapped in its memory space, as demonstrated by pdfunite. This can result in memory corruption and denial of service. This may be exploitable when a victim opens a specially crafted PDF file.			
postgresql -- postgresql	Privilege escalation flaws were found in the Red Hat initialization scripts of PostgreSQL. An attacker with access to the postgres user account could use these flaws to obtain root access on the server machine.	2018-07-27	Aún sin calcular	CVE-2017-15097 SECTRACK REDHAT REDHAT REDHAT REDHAT CONFIRM
powerdns -- recursor	An issue has been found in the parsing of authoritative answers in PowerDNS Recursor before 4.0.8, leading to a NULL pointer dereference when parsing a specially crafted answer containing a CNAME of a different class than IN. An unauthenticated remote attacker could cause a denial of service.	2018-07-27	Aún sin calcular	CVE-2017-15120 MLIST CONFIRM CONFIRM DEBIAN
pydio -- pydio	Pydio version 8.2.0 and earlier contains a Cross Site Scripting (XSS) vulnerability in ./core/vendor/meenie/javascript-packer/example-inline.php line 48; ./core/vendor/dapphp/securimage/examples/test.mysql.static.php lines: 114,118 that can result in an unauthenticated remote attacker manipulating the web client via XSS code injection. This attack appear to be exploitable via the victim openning a specially crafted URL. This vulnerability appears to have been fixed in version 8.2.1.	2018-07-23	Aún sin calcular	CVE-2018-1999016 CONFIRM MISC
pydio -- pydio	Pydio version 8.2.1 and prior contains an Unvalidated user input leading to Remote Code Execution (RCE) vulnerability in plugins/action.antivirus/AntivirusScanner.php: Line 124, scanNow($nodeObject) that can result in An attacker gaining admin access and can then execute arbitrary commands on the underlying OS. This attack appear to be exploitable via The attacker edits the Antivirus Command in the antivirus plugin, and executes the payload by uploading any file within Pydio.	2018-07-23	Aún sin calcular	CVE-2018-1999018 MISC
pydio -- pydio	Pydio version 8.2.0 and earlier contains a Server-Side Request Forgery (SSRF) vulnerability in	2018-07-23	Aún sin calcular	CVE-2018-1999017 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	plugins/action.updater/UpgradeManager.php Line: 154, getUpgradePath($url) that can result in an authenticated admin users requesting arbitrary URL's, pivoting requests through the server. This attack appears to be exploitable via the attacker gaining access to an administrative account, enters a URL into Upgrade Engine, and reloads the page or presses "Check Now". This vulnerability appears to have been fixed in 8.2.1.			
qemu -- qemu	An out-of-bounds memory access issue was found in Quick Emulator (QEMU) before 1.7.2 in the VNC display driver. This flaw could occur while refreshing the VNC display surface area in the 'vnc_refresh_server_surface'. A user inside a guest could use this flaw to crash the QEMU process.	2018-07-27	Aún sin calcular	CVE-2017-2633 MLIST BID REDHAT REDHAT REDHAT REDHAT CONFIRM CONFIRM CONFIRM
qemu -- qemu	A heap buffer overflow flaw was found in QEMU's Cirrus CLGD 54xx VGA emulator's VNC display driver support before 2.9; the issue could occur when a VNC client attempted to update its display after a VGA operation is performed by a guest. A privileged user/process inside a guest could use this flaw to crash the QEMU process or, potentially, execute arbitrary code on the host with privileges of the QEMU process.	2018-07-27	Aún sin calcular	CVE-2016-9603 BID SECTRACK REDHAT REDHAT REDHAT REDHAT REDHAT REDHAT REDHAT REDHAT REDHAT REDHAT REDHAT CONFIRM MLIST GENTOO CONFIRM
qemu -- qemu	Quick emulator (QEMU) before 2.8 built with the Cirrus CLGD 54xx VGA Emulator support is vulnerable to an out-of-bounds access issue. The issue could occur while copying VGA data in cirrus_bitblt_cputovideo. A privileged user inside guest could use this flaw to crash the QEMU process OR potentially execute arbitrary code on host with privileges of the QEMU process.	2018-07-27	Aún sin calcular	CVE-2017-2620 REDHAT REDHAT REDHAT REDHAT REDHAT REDHAT REDHAT REDHAT REDHAT

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				REDHAT REDHAT REDHAT MLIST BID SECTRACK CONFIRM MLIST MLIST GENTOO GENTOO CONFIRM CONFIRM
qemu -- qemu	The Network Block Device (NBD) server in Quick Emulator (QEMU) before 2.11 is vulnerable to a denial of service issue. It could occur if a client sent large option requests, making the server waste CPU time on reading up to 4GB per request. A client could use this flaw to keep the NBD server from serving other requests, resulting in DoS.	2018-07-27	Aún sin calcular	CVE-2017-15119 MISC BID REDHAT REDHAT CONFIRM MISC UBUNTU DEBIAN
qemu -- qemu	A stack buffer overflow flaw was found in the Quick Emulator (QEMU) before 2.9 built with the Network Block Device (NBD) client support. The flaw could occur while processing server's response to a 'NBD_OPT_LIST' request. A malicious NBD server could use this issue to crash a remote NBD client resulting in DoS or potentially execute arbitrary code on client host with privileges of the QEMU process.	2018-07-27	Aún sin calcular	CVE-2017-2630 MLIST BID REDHAT CONFIRM MLIST GENTOO
qemu -- qemu	A stack-based buffer overflow vulnerability was found in NBD server implementation in qemu before 2.11 allowing a client to request an export name of size up to 4096 bytes, which in fact should be limited to 256 bytes, causing an out-of-bounds stack write in the qemu process. If NBD server requires TLS, the attacker cannot trigger the buffer overflow without first successfully negotiating TLS.	2018-07-27	Aún sin calcular	CVE-2017-15118 MISC BID REDHAT CONFIRM MISC UBUNTU EXPLOIT-DB
qemu -- qemu	An assertion-failure flaw was found in Qemu before 2.10.1, in the Network Block Device (NBD) server's initial connection negotiation, where the I/O coroutine was undefined. This could crash the qemu-nbd server if a client	2018-07-26	Aún sin calcular	CVE-2017-7539 MLIST BID REDHAT REDHAT

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	sent unexpected data during connection negotiation. A remote user or process could use this flaw to crash the qemu-nbd server resulting in denial of service.			REDHAT REDHAT REDHAT REDHAT REDHAT CONFIRM CONFIRM CONFIRM
quazip -- quazip	QuaZIP before 0.7.6 is vulnerable to directory traversal, allowing attackers to write to arbitrary files via a ../ (dot dot slash) in a Zip archive entry that is mishandled during extraction. This vulnerability is also known as 'Zip-Slip'.	2018-07-25	Aún sin calcular	CVE-2018-1002209 MISC CONFIRM CONFIRM MISC
quick_heal -- multiple_products	Quick Heal Total Security 64 bit 17.00 (QHTS64.exe), (QHTSFT64.exe) - Version 10.0.1.38; Quick Heal Total Security 32 bit 17.00 (QHTS32.exe), (QHTSFT32.exe) - Version 10.0.1.38; Quick Heal Internet Security 64 bit 17.00 (QHIS64.exe), (QHISFT64.exe) - Version 10.0.0.37; Quick Heal Internet Security 32 bit 17.00 (QHIS32.exe), (QHISFT32.exe) - Version 10.0.0.37; Quick Heal AntiVirus Pro 64 bit 17.00 (QHAV64.exe), (QHAVFT64.exe) - Version 10.0.0.37; and Quick Heal AntiVirus Pro 32 bit 17.00 (QHAV32.exe), (QHAVFT32.exe) - Version 10.0.0.37 allow DLL Hijacking because of Insecure Library Loading.	2018-07-25	Aún sin calcular	CVE-2018-8090 MISC
red_hat -- certificate_system	An input validation error was found in Red Hat Certificate System's handling of client provided certificates before 8.1.20-1. If the certreq field is not present in a certificate an assertion error is triggered causing a denial of service.	2018-07-26	Aún sin calcular	CVE-2017-7509 SECTRACK REDHAT CONFIRM
red_hat -- cloudforms	A number of unused delete routes are present in CloudForms before 5.7.2.1 which can be accessed via GET requests instead of just POST requests. This could allow an attacker to bypass the protect_from_forgery XSRF protection causing the routes to be used. This attack would require additional cross-site scripting or similar attacks in order to execute.	2018-07-27	Aún sin calcular	CVE-2017-2653 BID REDHAT CONFIRM
red_hat -- cloudforms	A flaw was found in CloudForms before 5.9.0.22 in the self-service UI snapshot	2018-07-27	Aún sin calcular	CVE-2017-15125 BID

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	feature where the name field is not properly sanitized for HTML and JavaScript input. An attacker could use this flaw to execute a stored XSS attack on an application administrator using CloudForms. Please note that CSP (Content Security Policy) prevents exploitation of this XSS however not all browsers support CSP.			REDHAT CONFIRM
red_hat -- cloudforms	The dialog for creating cloud volumes (cinder provider) in CloudForms does not filter cloud tenants by user. An attacker with the ability to create storage volumes could use this to create storage volumes for any other tenant.	2018-07-27	Aún sin calcular	CVE-2017-7497 REDHAT REDHAT CONFIRM
red_hat -- cloudforms	It was found that CloudForms does not verify that the server hostname matches the domain name in the certificate when using a custom CA and communicating with Red Hat Virtualization (RHEV) and OpenShift. This would allow an attacker to spoof RHEV or OpenShift systems and potentially harvest sensitive information from CloudForms.	2018-07-27	Aún sin calcular	CVE-2017-2639 BID SECTRACK REDHAT CONFIRM
red_hat -- cloudforms	A logic error in valid_role() in CloudForms role validation before 5.7.1.3 could allow a tenant administrator to create groups with a higher privilege level than the tenant administrator should have. This would allow an attacker with tenant administration access to elevate privileges.	2018-07-27	Aún sin calcular	CVE-2017-2632 REDHAT BID CONFIRM
red_hat -- cloudforms_management_engine	CloudForms Management Engine (cfme) is vulnerable to an improper security setting in the dRuby component of CloudForms. An attacker with access to an unprivileged local shell could use this flaw to execute commands as a high privileged user.	2018-07-24	Aún sin calcular	CVE-2018-10905 CONFIRM
red_hat -- cloudforms_management_engine	CloudForms Management Engine (cfme) before 5.7.3 and 5.8.x before 5.8.1 lacks RBAC controls on certain methods in the rails application portion of CloudForms. An attacker with access could use a variety of methods within the rails application portion of CloudForms to escalate privileges.	2018-07-26	Aún sin calcular	CVE-2017-2664 BID REDHAT REDHAT CONFIRM
red_hat -- cloudforms_management_engine	In CloudForms Management Engine (cfme) before 5.7.3 and 5.8.x before 5.8.1, it was found that privilege check is missing when invoking arbitrary methods via filtering on VMs that MiqExpression will execute that is	2018-07-26	Aún sin calcular	CVE-2017-7530 BID REDHAT CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	triggerable by API users. An attacker could use this to execute actions they should not be allowed to (e.g. destroying VMs).			
red_hat -- enterprise_linux	A regression was found in the Red Hat Enterprise Linux 6.9 version of httpd 2.2.15-60, causing comments in the "Allow" and "Deny" configuration lines to be parsed incorrectly. A web administrator could unintentionally allow any client to access a restricted HTTP resource.	2018-07-26	Aún sin calcular	CVE-2017-12171 BID SECTRACK REDHAT CONFIRM
red_hat -- enterprise_linux	It was found that sssd's sysdb_search_user_by_upn_res() function before 1.16.0 did not sanitize requests when querying its local cache and was vulnerable to injection. In a centralized login environment, if a password hash was locally cached for a given user, an authenticated attacker could use this flaw to retrieve it.	2018-07-27	Aún sin calcular	CVE-2017-12173 REDHAT REDHAT CONFIRM
red_hat -- enterprise_linux	It was discovered that rpm-ostree and rpm-ostree-client before 2017.3 fail to properly check GPG signatures on packages when doing layering. Packages with unsigned or badly signed content could fail to be rejected as expected. This issue is partially mitigated on RHEL Atomic Host, where certificate pinning is used by default.	2018-07-27	Aún sin calcular	CVE-2017-2623 BID REDHAT CONFIRM
red_hat -- enterprise_linux _server	It was found that a mock CMC authentication plugin with a hardcoded secret was accidentally enabled by default in the pki-core package before 10.6.4. An attacker could potentially use this flaw to bypass the regular authentication process and trick the CA server into issuing certificates.	2018-07-26	Aún sin calcular	CVE-2017-7537 REDHAT CONFIRM CONFIRM
red_hat -- jboss_bpm_suite _and_jboss_data _virtualization_a nd_services	It was discovered that the Dashbuilder login page as used in Red Hat JBoss BPM Suite before 6.4.2 and Red Hat JBoss Data Virtualization & Services before 6.4.3 could be opened in an IFRAME, which made it possible to intercept and manipulate requests. An attacker could use this flaw to trick a user into performing arbitrary actions in the Console (clickjacking).	2018-07-27	Aún sin calcular	CVE-2017-2658 REDHAT BID REDHAT CONFIRM
red_hat -- jboss_brms_and _bpm_suite	JBoss BRMS 6 and BPM Suite 6 before 6.4.3 are vulnerable to a stored XSS via several lists in Business Central. The flaw is due to lack of sanitation of user input when	2018-07-27	Aún sin calcular	CVE-2017-2674 BID REDHAT REDHAT

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	creating new lists. Remote, authenticated attackers that have privileges to create lists can store scripts in them, which are not properly sanitized before showing to other users, including admins.			CONFIRM
red_hat -- jboss_brms_and_bpm_suite	JBoss BRMS 6 and BPM Suite 6 before 6.4.3 are vulnerable to a reflected XSS via artifact upload. A malformed XML file, if uploaded, causes an error message to appear that includes part of the bad XML code verbatim without filtering out scripts. Successful exploitation would allow execution of script code within the context of the affected user.	2018-07-27	Aún sin calcular	CVE-2017-7463 BID REDHAT REDHAT CONFIRM
red_hat -- jboss_eap	It was found that the JAXP implementation used in JBoss EAP 7.0 for SAX and DOM parsing is vulnerable to certain XXE flaws. An attacker could use this flaw to cause DoS, SSRF, or information disclosure if they are able to provide XML content for parsing.	2018-07-27	Aún sin calcular	CVE-2017-7464 BID CONFIRM
red_hat -- jboss_enterprise_application	It was found that the log file viewer in Red Hat JBoss Enterprise Application 6 and 7 allows arbitrary file read to authenticated user via path traversal.	2018-07-27	Aún sin calcular	CVE-2017-2595 REDHAT REDHAT BID SECTRACK REDHAT REDHAT REDHAT REDHAT REDHAT REDHAT REDHAT REDHAT REDHAT REDHAT REDHAT CONFIRM
red_hat -- jboss_fuse	It was discovered that the hawtio servlet 1.4 uses a single HttpClient instance to proxy requests with a persistent cookie store (cookies are stored locally and are not passed between the client and the end URL) which means all clients using that proxy are sharing the same cookies.	2018-07-26	Aún sin calcular	CVE-2017-2589 REDHAT CONFIRM
red_hat -- openstack_platform	A design flaw issue was found in the Red Hat OpenStack Platform director use of TripleO to enable libvirtd based live-migration. Libvirtd is deployed by default (by director)	2018-07-26	Aún sin calcular	CVE-2017-2637 BID REDHAT REDHAT

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	listening on 0.0.0.0 (all interfaces) with no-authentication or encryption. Anyone able to make a TCP connection to any compute host IP address, including 127.0.0.1, other loopback interface addresses, or in some cases possibly addresses that have been exposed beyond the management interface, could use this to open a virsh session to the libvirtd instance and gain control of virtual machine instances or possibly take over the host.			REDHAT REDHAT CONFIRM CONFIRM CONFIRM
red_hat -- satellite	Red Hat Satellite before 6.5 is vulnerable to a XSS in discovery rule when you are entering filter and you use autocomplete functionality.	2018-07-26	Aún sin calcular	CVE-2017-12175 BID CONFIRM CONFIRM
red_hat -- satellite	A cross-site scripting (XSS) flaw was found in how an organization name is displayed in Satellite 5, before 5.8. A user able to change an organization's name could exploit this flaw to perform XSS attacks against other Satellite users.	2018-07-26	Aún sin calcular	CVE-2017-7538 SECTRACK REDHAT CONFIRM
red_hat -- spacewalk-channel	It was found that spacewalk-channel can be used by a non-admin user or disabled users to perform administrative tasks due to an incorrect authorization check in backend/server/rhnChannel.py.	2018-07-27	Aún sin calcular	CVE-2017-7470 BID REDHAT CONFIRM
red_hat -- undertow	It was discovered that Undertow before 1.4.17, 1.3.31 and 2.0.0 processes http request headers with unusual whitespaces which can cause possible http request smuggling.	2018-07-27	Aún sin calcular	CVE-2017-12165 REDHAT REDHAT REDHAT REDHAT REDHAT REDHAT REDHAT REDHAT REDHAT CONFIRM
red_hat -- undertow	It was found in Undertow before 1.3.28 that with non-clean TCP close, the Websocket server gets into infinite loop on every IO thread, effectively causing DoS.	2018-07-27	Aún sin calcular	CVE-2017-2670 REDHAT BID REDHAT REDHAT REDHAT REDHAT REDHAT REDHAT REDHAT

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				CONFIRM DEBIAN
red_hat -- undertow	It was discovered in Undertow that the code that parsed the HTTP request line permitted invalid characters. This could be exploited, in conjunction with a proxy that also permitted the invalid characters but with a different interpretation, to inject data into the HTTP response. By manipulating the HTTP response the attacker could poison a web-cache, perform an XSS attack, or obtain sensitive information from requests other than their own.	2018-07-27	Aún sin calcular	CVE-2017-2666 REDHAT BID REDHAT REDHAT REDHAT REDHAT REDHAT REDHAT REDHAT CONFIRM DEBIAN
red_hat -- virtualization	When updating a password in the rhvm database the ovirt-aaa-jdbc-tool tools before 1.1.3 fail to correctly check for the current password if it is expired. This would allow access to an attacker with access to change the password on accounts with expired passwords, gaining access to those accounts.	2018-07-27	Aún sin calcular	CVE-2017-2614 REDHAT CONFIRM
redhat -- openstack-neutron	A race-condition flaw was discovered in openstack-neutron before 7.2.0-12.1, 8.x before 8.3.0-11.1, 9.x before 9.3.1-2.1, and 10.x before 10.0.2-1.1, where, following a minor overcloud update, neutron security groups were disabled. Specifically, the following were reset to 0: net.bridge.bridge-nf-call-ip6tables and net.bridge.bridge-nf-call-iptables. The race was only triggered by an update, at which point an attacker could access exposed tenant VMs and network resources.	2018-07-26	Aún sin calcular	CVE-2017-7543 BID REDHAT REDHAT REDHAT REDHAT REDHAT REDHAT CONFIRM
redhat -- openstack_orchestration	An access-control flaw was found in the OpenStack Orchestration (heat) service before 8.0.0, 6.1.0 and 7.0.2 where a service log directory was improperly made world readable. A malicious system user could exploit this flaw to access sensitive information.	2018-07-27	Aún sin calcular	CVE-2017-2621 BID REDHAT REDHAT CONFIRM
redhat -- openstack_workflow	An accessibility flaw was found in the OpenStack Workflow (mistral) service where a service log directory was improperly made world readable. A malicious system user could exploit this flaw to access sensitive information.	2018-07-27	Aún sin calcular	CVE-2017-2622 REDHAT CONFIRM
rsa -- archer	RSA Archer, versions prior to 6.4.0.1, contain	2018-07-24	Aún sin calcular	CVE-2018-11059

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	a stored cross-site scripting vulnerability. A remote authenticated malicious Archer user could potentially exploit this vulnerability to store malicious HTML or JavaScript code in a trusted application data store. When application users access the corrupted data store through their browsers, the malicious code gets executed by the web browser in the context of the vulnerable web application.			FULLDISC BID SECTRACK
rsa -- archer	RSA Archer, versions prior to 6.4.0.1, contain an authorization bypass vulnerability in the REST API. A remote authenticated malicious Archer user could potentially exploit this vulnerability to elevate their privileges.	2018-07-24	Aún sin calcular	CVE-2018-11060 FULLDISC BID SECTRACK
sage -- xrt_treasury	Sage XRT Treasury, version 3, fails to properly restrict database access to authorized users, which may enable any authenticated user to gain full access to privileged database functions. Sage XRT Treasury is a business finance management application. Database user access privileges are determined by the USER_CODE field associated with the querying user. By modifying the USER_CODE value to match that of a privileged user, a low-privileged, authenticated user may gain privileged access to the SQL database. A remote, authenticated user can submit specially crafted SQL queries to gain privileged access to the application database.	2018-07-24	Aún sin calcular	CVE-2017-3183 CERT-VN BID
samba -- samba	A flaw was found in the way samba client before samba 4.4.16, samba 4.5.14 and samba 4.6.8 used encryption with the max protocol set as SMB3. The connection could lose the requirement for signing and encrypting to any DFS redirects, allowing an attacker to read or alter the contents of the connection via a man-in-the-middle attack.	2018-07-27	Aún sin calcular	CVE-2017-12151 BID SECTRACK REDHAT REDHAT CONFIRM CONFIRM CONFIRM CONFIRM DEBIAN CONFIRM
samba -- samba	An information leak flaw was found in the way SMB1 protocol was implemented by Samba before 4.4.16, 4.5.x before 4.5.14, and 4.6.x before 4.6.8. A malicious client could use this flaw to dump server memory	2018-07-26	Aún sin calcular	CVE-2017-12163 BID SECTRACK REDHAT REDHAT

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	contents to a file on the samba share or to a shared printer, though the exact area of server memory cannot be controlled by the attacker.			REDHAT REDHAT CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM DEBIAN CONFIRM CONFIRM
samba -- samba	It was found that samba before 4.4.16, 4.5.x before 4.5.14, and 4.6.x before 4.6.8 did not enforce "SMB signing" when certain configuration options were enabled. A remote attacker could launch a man-in-the-middle attack and retrieve information in plain-text.	2018-07-26	Aún sin calcular	CVE-2017-12150 BID SECTRACK REDHAT REDHAT REDHAT REDHAT CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM DEBIAN CONFIRM
seacms -- seacms	SeaCMS 6.61 has two XSS issues in the admin_config.php file via certain form fields.	2018-07-23	Aún sin calcular	CVE-2018-14517 MISC
sel -- acselerator_architect	SEL AcSELerator Architect version 2.2.24.0 and prior can be exploited when the AcSELerator Architect FTP client connects to a malicious FTP server, which may cause denial of service via 100% CPU utilization. Restart of the application is required.	2018-07-24	Aún sin calcular	CVE-2018-10608 MISC
sel -- acselerator_architect	SEL AcSELerator Architect version 2.2.24.0 and prior allows unsanitized input to be passed to the XML parser, which may allow disclosure and retrieval of arbitrary data, arbitrary code execution (in certain situations on specific platforms), and denial of service attacks.	2018-07-24	Aún sin calcular	CVE-2018-10600 MISC
sel -- compass	SEL Compass version 3.0.5.1 and prior allows all users full access to the SEL Compass directory, which may allow modification or overwriting of files within the Compass installation folder, resulting in escalation of privilege and/or malicious code execution.	2018-07-24	Aún sin calcular	CVE-2018-10604 MISC
sharpcompress --	SharpCompress before 0.21.0 is vulnerable to directory traversal, allowing attackers to	2018-07-25	Aún sin calcular	CVE-2018-1002206 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sharpcompress	write to arbitrary files via a ../ (dot dot slash) in a Zip archive entry that is mishandled during extraction. This vulnerability is also known as 'Zip-Slip'.			CONFIRM MISC MISC MISC
sharplibzip -- sharplibzip	sharplibzip before 1.0 RC1 is vulnerable to directory traversal, allowing attackers to write to arbitrary files via a ../ (dot dot slash) in a Zip archive entry that is mishandled during extraction. This vulnerability is also known as 'Zip-Slip'.	2018-07-25	Aún sin calcular	CVE-2018-1002208 CONFIRM CONFIRM MISC MISC MISC
siemens -- ethernet_modules	A vulnerability has been identified in Firmware variant IEC 61850 for EN100 Ethernet module (All versions < V4.33), Firmware variant PROFINET IO for EN100 Ethernet module (All versions), Firmware variant Modbus TCP for EN100 Ethernet module (All versions), Firmware variant DNP3 TCP for EN100 Ethernet module (All versions), Firmware variant IEC104 for EN100 Ethernet module (All versions). Specially crafted packets to port 102/tcp could cause a denial-of-service condition in the EN100 communication module if oscillographs are running. A manual restart is required to recover the EN100 module functionality. Successful exploitation requires an attacker with network access to send multiple packets to the EN100 module. As a precondition the IEC 61850-MMS communication needs to be activated on the affected EN100 modules. No user interaction or privileges are required to exploit the security vulnerability. The vulnerability could allow causing a Denial-of-Service condition of the network functionality of the device, compromising the availability of the system. At the time of advisory publication no public exploitation of this security vulnerability was known.	2018-07-23	Aún sin calcular	CVE-2018-11452 CONFIRM
siemens -- ethernet_modules	A vulnerability has been identified in Firmware variant IEC 61850 for EN100 Ethernet module (All versions < V4.33), Firmware variant PROFINET IO for EN100 Ethernet module (All versions), Firmware variant Modbus TCP for EN100 Ethernet module (All versions), Firmware variant DNP3 TCP for EN100 Ethernet module (All versions), Firmware variant IEC104 for	2018-07-23	Aún sin calcular	CVE-2018-11451 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	EN100 Ethernet module (All versions), SIPROTEC 5 relays with CPU variants CP300 and CP100 and the respective Ethernet communication modules (All versions < V7.80), SIPROTEC 5 relays with CPU variants CP200 and the respective Ethernet communication modules (All versions). Specially crafted packets to port 102/tcp could cause a denial-of-service condition in the affected products. A manual restart is required to recover the EN100 module functionality of SIPROTEC 4 and SIPROTEC Compact relays. Successful exploitation requires an attacker with network access to send multiple packets to the affected products or modules. As a precondition the IEC 61850-MMS communication needs to be activated on the affected products or modules. No user interaction or privileges are required to exploit the vulnerability. The vulnerability could allow causing a Denial-of-Service condition of the network functionality of the device, compromising the availability of the system. At the time of advisory publication no public exploitation of this security vulnerability was known.			
sourcetree -- sourcetree	There was an argument injection vulnerability in Sourcetree for macOS via filenames in Mercurial repositories. An attacker with permission to commit to a Mercurial repository linked in Sourcetree for macOS is able to exploit this issue to gain code execution on the system. Versions of Sourcetree for macOS from 1.0b2 before 2.7.6 are affected by this vulnerability.	2018-07-24	Aún sin calcular	CVE-2018-13385 CONFIRM
sourcetree -- sourcetree	There was an argument injection vulnerability in Sourcetree for Windows via filenames in Mercurial repositories. An attacker with permission to commit to a Mercurial repository linked in Sourcetree for Windows is able to exploit this issue to gain code execution on the system. Versions of Sourcetree for Windows before version 2.6.9 are affected by this vulnerability.	2018-07-24	Aún sin calcular	CVE-2018-13386 CONFIRM
spice -- spice	A vulnerability was discovered in SPICE before 0.13.90 in the server's protocol handling. An authenticated attacker could send crafted messages to the SPICE server	2018-07-27	Aún sin calcular	CVE-2016-9577 REDHAT REDHAT BID

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	causing a heap overflow leading to a crash or possible code execution.			REDHAT REDHAT CONFIRM DEBIAN
spice -- spice	A vulnerability was discovered in SPICE before 0.13.90 in the server's protocol handling. An attacker able to connect to the SPICE server could send crafted messages which would cause the process to crash.	2018-07-27	Aún sin calcular	CVE-2016-9578 REDHAT REDHAT BID REDHAT REDHAT CONFIRM DEBIAN
suricata -- suricata	An issue was discovered in Suricata before 3.1.2. If an ICMPv4 error packet is received as the first packet on a flow in the to_client direction, it confuses the rule grouping lookup logic. The toclient inspection will then continue with the wrong rule group. This can lead to missed detection.	2018-07-23	Aún sin calcular	CVE-2016-10728 MISC MISC MISC
suricata -- suricata	Suricata before 4.0.5 stops TCP stream inspection upon a TCP RST from a server. This allows detection bypass because Windows TCP clients proceed with normal processing of TCP data that arrives shortly after an RST (i.e., they act as if the RST had not yet been received).	2018-07-23	Aún sin calcular	CVE-2018-14568 MISC MISC MISC MISC
symantec -- management_agent	The Inventory Plugin for Symantec Management Agent prior to 7.6 POST HF7, 8.0 POST HF6, or 8.1 RU7 may be susceptible to a privilege escalation vulnerability, which is a type of issue that allows a user to gain elevated access to resources that are normally protected at lower access levels.	2018-07-25	Aún sin calcular	CVE-2018-5240 BID CONFIRM
tenda -- ac7	Tenda AC7 through V15.03.06.44_CN, AC9 through V15.03.05.19(6318)_CN, and AC10 through V15.03.06.23_CN devices have a Stack-based Buffer Overflow via a long limitSpeed or limitSpeedup parameter to an unspecified /goform URI.	2018-07-21	Aún sin calcular	CVE-2018-14492 MISC
thomson_reuters -- ultratax_cs	Thomson Reuters UltraTax CS 2017 on Windows, in a client/server configuration, transfers customer records and bank account numbers in cleartext over SMBv2, which allows attackers to (1) obtain sensitive information by sniffing the network or (2) conduct man-in-the-middle (MITM) attacks via unspecified vectors. The customer record	2018-07-26	Aún sin calcular	CVE-2018-14607 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	transferred in cleartext contains: Client ID, Full Name, Spouse's Full Name, Social Security Number, Spouse's Social Security Number, Occupation, Spouse's Occupation, Daytime Phone, Home Phone, Tax Preparer, Federal and State Taxes to File, Bank Name, Bank Account Number, and possibly other sensitive information.			
thomson_reuters -- ultratax_cs	Thomson Reuters UltraTax CS 2017 on Windows has a password protection option; however, the level of protection might be inconsistent with some customers' expectations because the data is directly accessible in cleartext. Specifically, it stores customer data in unique directories (%install_path%\WinCSI\UT17DATA\client_ID\file_name.XX17) that can be bypassed without authentication by examining the strings of the .XX17 file. The strings stored in the .XX17 file contain each customer's: Full Name, Spouse's Name, Social Security Number, Date of Birth, Occupation, Home Address, Daytime Phone Number, Home Phone Number, Spouse's Address, Spouse's Daytime Phone Number, Spouse's Social Security Number, Spouse's Home Phone Number, Spouse's Occupation, Spouse's Date of Birth, and Spouse's Filing Status.	2018-07-26	Aún sin calcular	CVE-2018-14608 MISC
threatmetrix -- threatmetrix_sdk	On the iOS platform, the ThreatMetrix SDK versions prior to 3.2 fail to validate SSL certificates provided by HTTPS connections, which may allow an attacker to perform a man-in-the-middle (MITM) attack. ThreatMetrix is a security library for mobile applications, which aims to provide fraud prevention and device identity capabilities. The ThreatMetrix SDK versions prior to 3.2 do not validate SSL certificates on the iOS platform. An affected application will communicate with https://h-sdk.online-metrix.net, regardless of whether the connection is secure or not. An attacker on the same network as or upstream from the iOS device may be able to view or modify ThreatMetrix network traffic that should have been protected by HTTPS.	2018-07-24	Aún sin calcular	CVE-2017-3182 CERT-VN BID
thulac -- thulac	An issue was discovered in libthulac.so in THULAC through 2018-02-25. A heap-based	2018-07-23	Aún sin calcular	CVE-2018-14565 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	buffer over-read can occur in NGramFeature::find_bases in include/cb_ngram_feature.h.			
thulac -- thulac	An issue was discovered in libthulac.so in THULAC through 2018-02-25. A SEGV can occur in NGramFeature::find_bases in include/cb_ngram_feature.h.	2018-07-23	Aún sin calcular	CVE-2018-14564 MISC
thulac -- thulac	An issue was discovered in libthulac.so in THULAC through 2018-02-25. "operator delete" is used with "operator new[]" in the TaggingLearner class in include/cb_tagging_learner.h, possibly leading to memory corruption.	2018-07-23	Aún sin calcular	CVE-2018-14563 MISC
thulac -- thulac	An issue was discovered in libthulac.so in THULAC through 2018-02-25. A NULL pointer dereference can occur in the BasicModel class in include/cb_model.h.	2018-07-23	Aún sin calcular	CVE-2018-14562 MISC
tibco -- multiple_products	Multiple TIBCO Products are prone to multiple unspecified cross-site scripting vulnerabilities because it fails to properly sanitize user-supplied input. An attacker may leverage these issues to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This can allow the attacker to steal cookie-based authentication credentials and to launch other attacks. The products and versions that are affected include the following: TIBCO Silver Fabric Enabler for Spotfire Web Player 2.1.2 and earlier TIBCO Spotfire Analyst 7.5.0 TIBCO Spotfire Analyst 7.6.0 TIBCO Spotfire Analyst 7.7.0 TIBCO Spotfire Analytics Platform for AWS Marketplace 7.0.2 and earlier TIBCO Spotfire Automation Services 6.5.3 and earlier TIBCO Spotfire Automation Services 7.0.0, and 7.0.1 TIBCO Spotfire Connectors 7.6.0 TIBCO Spotfire Deployment Kit 6.5.3 and earlier TIBCO Spotfire Deployment Kit 7.0.0, and 7.0.1 TIBCO Spotfire Deployment Kit 7.5.0 TIBCO Spotfire Deployment Kit 7.6.0 TIBCO Spotfire Deployment Kit 7.7.0 TIBCO Spotfire Desktop 6.5.2 and earlier TIBCO Spotfire Desktop 7.0.0, and 7.0.1 TIBCO Spotfire Desktop 7.5.0 TIBCO Spotfire Desktop 7.6.0 TIBCO Spotfire Desktop 7.7.0 TIBCO Spotfire Desktop Developer Edition	2018-07-24	Aún sin calcular	CVE-2017-3180 BID CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	7.7.0 TIBCO Spotfire Desktop Language Packs 7.0.1 and earlier TIBCO Spotfire Desktop Language Packs 7.5.0 TIBCO Spotfire Desktop Language Packs 7.6.0 TIBCO Spotfire Desktop Language Packs 7.7.0 TIBCO Spotfire Professional 6.5.3 and earlier TIBCO Spotfire Professional 7.0.0 and 7.0.1 TIBCO Spotfire Web Player 6.5.3 and earlier TIBCO Spotfire Web Player 7.0.0 and 7.0.1			
tibco -- multiple_products	Multiple TIBCO Products are prone to multiple unspecified SQL-injection vulnerabilities because it fails to properly sanitize user-supplied input before using it in an SQL query. Exploiting these issues could allow an attacker to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database. The following products and versions are affected: TIBCO Spotfire Analyst 7.7.0 TIBCO Spotfire Connectors 7.6.0 TIBCO Spotfire Deployment Kit 7.7.0 TIBCO Spotfire Desktop 7.6.0 TIBCO Spotfire Desktop 7.7.0 TIBCO Spotfire Desktop Developer Edition 7.7.0 TIBCO Spotfire Desktop Language Packs 7.6.0 TIBCO Spotfire Desktop Language Packs 7.7.0 The following components are affected: TIBCO Spotfire Client TIBCO Spotfire Web Player Client	2018-07-24	Aún sin calcular	CVE-2017-3181 BID CONFIRM
tightrope_media -- carousel_digital_signage	A Local File Inclusion (LFI) vulnerability exists in the Web Interface API of TightRope Media Carousel Digital Signage before 7.3.5. The RenderingFetch API allows for the downloading of arbitrary files through the use of directory traversal sequences, aka CSL-1683.	2018-07-23	Aún sin calcular	CVE-2018-14573 CONFIRM
vmware -- esxi_and_workstation_and_fusion	VMware ESXi (6.7 before ESXi670-201806401-BG, 6.5 before ESXi650-201806401-BG, 6.0 before ESXi600-201806401-BG and 5.5 before ESXi550-201806401-BG), Workstation (14.x before 14.1.2), and Fusion (10.x before 10.1.2) contain a denial-of-service vulnerability due to NULL pointer dereference issue in RPC handler. Successful exploitation of this issue may allow attackers with normal user privileges to crash their VMs.	2018-07-25	Aún sin calcular	CVE-2018-6972 BID SECTRACK SECTRACK CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
vmware -- horizon_view_agents	VMware Horizon View Agents (7.x.x before 7.5.1) contain a local information disclosure vulnerability due to insecure logging of credentials in the vmmsi.log file when an account other than the currently logged on user is specified during installation (including silent installations). Successful exploitation of this issue may allow low privileged users access to the credentials specified during the Horizon View Agent installation.	2018-07-25	Aún sin calcular	CVE-2018-6971 BID SECTRACK SECTRACK CONFIRM
wancms -- wancms	wancms 1.0 through 5.0 allows remote attackers to cause a denial of service (resource consumption) via a checkcode (aka verification code) URI in which the values of font_size, width, and height are large numbers.	2018-07-25	Aún sin calcular	CVE-2018-14596 MISC
wesnoth -- battle_for_wesnoth	The Battle for Wesnoth Project version 1.7.0 through 1.14.3 contains a Code Injection vulnerability in the Lua scripting engine that can result in code execution outside the sandbox. This attack appear to be exploitable via Loading specially-crafted saved games, networked games, replays, and player content.	2018-07-23	Aún sin calcular	CVE-2018-1999023 CONFIRM
wildfly -- core	WildFly Core before version 6.0.0.Alpha3 does not properly validate file paths in .war archives, allowing for the extraction of crafted .war archives to overwrite arbitrary files. This is an instance of the 'Zip Slip' vulnerability.	2018-07-27	Aún sin calcular	CVE-2018-10862 REDHAT REDHAT REDHAT CONFIRM MISC
wizkunde -- samlbase	Wizkunde SAMLBase may incorrectly utilize the results of XML DOM traversal and canonicalization APIs in such a way that an attacker may be able to manipulate the SAML data without invalidating the cryptographic signature, allowing the attack to potentially bypass authentication to SAML service providers.	2018-07-24	Aún sin calcular	CVE-2018-5387 MISC CERT-VN
wordpress -- wordpress	The Mondula Multi Step Form plugin through 1.2.5 for WordPress allows XSS via the fw_data [id][1], fw_data [id][2], fw_data [id][3], fw_data [id][4], or email field of the contact form, exploitable with an fw_send_email action to wp-admin/admin-ajax.php.	2018-07-25	Aún sin calcular	CVE-2018-14430 MISC
wuzhi -- cms	A SQL injection was discovered in WUZHI CMS 4.1.0 that allows remote attackers to	2018-07-23	Aún sin calcular	CVE-2018-14515 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	inject a malicious SQL statement via the index.php?m=promote&f=index&v=search keywords parameter.			
wuzhi -- cms	An XSS vulnerability was discovered in WUZHI CMS 4.1.0. There is persistent XSS that allows remote attackers to inject arbitrary web script or HTML via the form[content] parameter to the index.php?m=feedback&f=index&v=contact URI.	2018-07-23	Aún sin calcular	CVE-2018-14513 MISC
wuzhi -- cms	An XSS vulnerability was discovered in WUZHI CMS 4.1.0. There is persistent XSS that allows remote attackers to inject arbitrary web script or HTML via the form[nickname] parameter to the index.php?m=core&f=set&v=sendmail URI. When the administrator accesses the "system settings - mail server" screen, the XSS payload is triggered.	2018-07-23	Aún sin calcular	CVE-2018-14512 MISC
x.org -- x.org	It was found that xorg-x11-server before 1.19.0 including uses memcmp() to check the received MIT cookie against a series of valid cookies. If the cookie is correct, it is allowed to attach to the Xorg session. Since most memcmp() implementations return after an invalid byte is seen, this causes a time difference between a valid and invalid byte, which could allow an efficient brute force attack.	2018-07-27	Aún sin calcular	CVE-2017-2624 BID SECTRACK CONFIRM MLIST GENTOO GENTOO MISC
xiao5ucompany -- xiao5ucompany	Feedback.asp in Xiao5uCompany 1.7 has XSS because the XSS protection mechanism in Safe.asp is insufficient (for example, it considers SCRIPT and IMG elements, but does not consider VIDEO elements).	2018-07-23	Aún sin calcular	CVE-2018-14527 MISC
xycms -- xycms	system/edit_book.php in XYCMS 1.7 has stored XSS via a crafted add_do.php request, related to add_book.php.	2018-07-28	Aún sin calcular	CVE-2018-14686 MISC
xyhcms -- xyhcms	xyhai.php?s=/Auth/addUser in XYHCMS 3.5 allows CSRF to add a background administrator account.	2018-07-24	Aún sin calcular	CVE-2018-14583 MISC
zeroturnaround -- zt_zip	zt-zip before 1.13 is vulnerable to directory traversal, allowing attackers to write to arbitrary files via a ../ (dot dot slash) in a Zip archive entry that is mishandled during extraction. This vulnerability is also known as 'Zip-Slip'.	2018-07-25	Aún sin calcular	CVE-2018-1002201 MISC CONFIRM CONFIRM MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zip4j -- zip4j	zip4j before 1.3.3 is vulnerable to directory traversal, allowing attackers to write to arbitrary files via a ../ (dot dot slash) in a Zip archive entry that is mishandled during extraction. This vulnerability is also known as 'Zip-Slip'.	2018-07-25	Aún sin calcular	CVE-2018-1002202 MISC MISC MISC
zjonsson -- node-unzipper	unzipper npm library before 0.8.13 is vulnerable to directory traversal, allowing attackers to write to arbitrary files via a ../ (dot dot slash) in a Zip archive entry that is mishandled during extraction. This vulnerability is also known as 'Zip-Slip'.	2018-07-25	Aún sin calcular	CVE-2018-1002203 MISC CONFIRM CONFIRM MISC MISC
zte -- zxcdn-sns	SQL injection vulnerability in all versions prior to V4.01.01 of the ZTE ZXCDN-SNS product allows remote attackers to execute arbitrary SQL commands via the aoData parameter, resulting in the disclosure of database information.	2018-07-25	Aún sin calcular	CVE-2017-10936 CONFIRM
zte -- zxiptv-epg	All versions prior to V5.09.02.02T4 of the ZTE ZXIPTV-EPG product use the Java RMI service in which the servers use the Apache Commons Collections (ACC) library that may result in Java deserialization vulnerabilities. An unauthenticated remote attacker can exploit the vulnerabilities by sending a crafted RMI request to execute arbitrary code on the target host.	2018-07-25	Aún sin calcular	CVE-2017-10934 CONFIRM
zte -- zxiptv-ucm	SQL injection vulnerability in all versions prior to V2.01.05.09 of the ZTE ZXIPTV-UCM product allows remote attackers to execute arbitrary SQL commands via the opertype parameter, resulting in the disclosure of database information.	2018-07-25	Aún sin calcular	CVE-2017-10937 CONFIRM
zte -- zxr10_1800-2s	All versions prior to ZSRV2 V3.00.40 of the ZTE ZXR10 1800-2S products allow remote authenticated users to bypass the original password authentication protection to change other user's password.	2018-07-25	Aún sin calcular	CVE-2017-10935 CONFIRM