PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
Spring Framework Remote Code Execution Vulnerability - CVE-2018-1275	Spring Framework, versions 5.0 prior to 5.0.5 and versions 4.3 prior to 4.3.16 and older unsupported versions, allow applications to expose STOMP over WebSocket endpoints with a simple, in-memory STOMP broker through the spring-messaging module. A malicious user (or attacker) can craft a message to the broker that can lead to a remote code execution attack. This CVE addresses the partial fix for CVE-2018-1270 in the 4.3.x branch of the Spring Framework.	Version(s): <= 4.3 - 4.3.15, 5.0 - 5.0.4	Published - April 11, 2018 CVE-2018-1275 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1275 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1275
Juniper Junos Remote DoS or Code Execution Vulnerability -	Receipt of a specially crafted Connectionless Network Protocol (CLNP) datagram destined to an interface of a Junos OS device may result in a kernel crash or lead to remote code execution. Devices are only vulnerable to the specially crafted CLNP datagram if 'clns-routing' or ES-IS is explicitly configured. Devices with without CLNS enabled are not vulnerable to this issue. Devices with IS-IS configured on the interface are not vulnerable to this issue unless CLNS routing is also enabled. This issue only affects devices running Junos OS 15.1. Affected releases are Juniper Networks Junos OS: 15.1 versions prior to 15.1F5-S3, 15.1F6-S8, 15.1F7, 15.1R5; 15.1X49 versions prior to 15.1X49-D60; 15.1X53 versions prior to 15.1X53-D66, 15.1X53-D233, 15.1X53-D471. Earlier releases are unaffected by this vulnerability, and the issue has been resolved in Junos OS 16.1R1 and all subsequent releases.	Version(s): <= 15.1-15.1F5\-R2, 15.1X53-\-D233, 15.1X53\-D65, 15.1F7, 15.1X49-15.1X49\-D59, 15.1F6\-R8	Published - April 11, 2018 CVE-2018-0016 CVSS - 9.8 Vendor's Advisory - http://www.securityfocus.com/bid/103747 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0016 https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10844&cat=SIRT_1&actp=LIST
Corosync Cluster Engine Remote DoS Vulnerability - CVE-2018-1084	Corosync before version 2.4.4 is vulnerable to an integer overflow in exec/totemcrypto.c.	Version(s): <= 2.4.4	Published - April 12, 2018 SBV-84298 CVSS - 7.5 Vendor's Advisory - http://www.securityfocus.com/bid/103758 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1084 https://bugzilla.redhat.com/show_bug.cgi?id=1552830 http://corosync.github.io/corosync/
LibreOffice Local DoS or Other Vulnerability in Sw/source/filter/ww8/ww8toolbar.cxx - CVE-2018-10120	The SwCTBWrapper::Read function in sw/source/filter/ww8/ww8toolbar.cxx in LibreOffice before 5.4.6.1 and 6.x before 6.0.2.1 does not validate a customizations index, which allows remote attackers to cause a denial of service (heap-based buffer overflow with write access) or possibly have unspecified other impact via a crafted document that contains a certain Microsoft Word record.	Version(s): <= 5.4.6, 6 - 6.0.1	Published - April 16, 2018 CVE-2018-10120 CVSS - 8.4 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10120 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-10120 https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=6173 https://gerrit.libreoffice.org//c/49486/
WordPress Unspecified Vulnerability - CVE-2018-10100	Before WordPress 4.9.5, the redirection URL for the login page was not validated or sanitized if forced to use HTTPS.	Version(s): <= 4.9.5	Published - April 16, 2018 CVE-2018-10100 CVSS - 8.2 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10100 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-10100 https://codex.wordpress.org/Version_4.9.5
[cisco-sa-20180418-uscd] Cisco UCS Director Remote Information Disclosure or Unspecified Vulnerability - CVE-2018-0238	A vulnerability in the role-based resource checking functionality of the Cisco Unified Computing System (UCS) Director could allow an authenticated, remote attacker to view unauthorized information for any virtual machine in the UCS Director end-user portal and perform any permitted operations on any virtual machine. The permitted operations can be configured for the end user on the virtual machines with either of the following settings: The virtual machine is associated to a Virtual Data Center (VDC) that has an end user self-service policy attached to the VDC. The end user role has VM Management Actions settings configured under User Permissions. This is a global configuration, so all the virtual machines visible in the end-user portal will have the VM management actions available. The vulnerability is due to improper user authentication checks. An attacker could exploit this vulnerability by logging in to the UCS Director with a modified username and valid password. A successful exploit could allow the attacker to gain visibility into and perform actions against all virtual machines in the UCS Director end-user portal of the affected system. This vulnerability affects Cisco Unified Computing System (UCS) Director releases 6.0 and 6.5 prior to patch 3 that are in a default configuration. Cisco Bug IDs: CSCvh53501.	Version(s): <= 6.5(0.1), 6.5(0.0)	Published - April 18, 2018 CVE-2018-0238 CVSS - 9.1 Vendor's Advisory - http://www.securityfocus.com/bid/103919 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0238 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0238
Nagios XI <5.4.13 Core Config Manager SQL Injection Vulnerability - CVE-2018-8734	SQL injection vulnerability in the core config manager in Nagios XI 5.2.x through 5.4.x before 5.4.13 allows an attacker to execute arbitrary SQL commands via the selInfoKey1 parameter.	Version(s): <= 5.2.0 - 5.4.12	Published - April 18, 2018 CVE-2018-8734 CVSS - 9.1 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8734 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8734 https://assets.nagios.com/downloads/nagiosxi/CHANGES-5.TXT
phpMyAdmin 4.8.0 before 4.8.0-1 CSRF Vulnerability	phpMyAdmin 4.8.0 before 4.8.0-1 has CSRF, allowing an attacker to execute arbitrary SQL statements, related to js/db_operations.js, js/tbl_operations.js, libraries/classes/Operations.php, and sql.php.	Version(s): <= 4.8.0	Published - April 19, 2018 CVE-2018-10188 CVSS - 8.8 Vendor's Advisory - http://www.securityfocus.com/bid/103936 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10188 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-10188
OpenJDK 1.8.0 before 1.8.0.171 Remote Code Execution in Security - CVE-2018-2794	OpenJDK 1.8.0 before 1.8.0.171 allows a remote attacker to execute arbitrary code via a crafted JCEKS key store. This issue exists due to a flaw in the Security component.	Version(s): <= 1.8.0 - 1.8.170	Published - April 19, 2018 CVE-2018-2794 CVSS - 7.7 Vendor's Advisory - http://www.securityfocus.com/bid/103817 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-2794 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-2794
Microsoft Internet Explorer Remote Code Execution via a Crafted Office Document	Microsoft Internet Explorer through 11 allows a remote attacker to execute arbitrary code via a crafted Office document containing an embedded malicious web page.	Version(s): <= 6 - 11	Published - April 23, 2018 SBV-84698 CVSS - 7.8 Vendor's Advisory - https://isc.sans.edu/diary/23581 https://mspoweruser.com/new-zero-day-double-kill-malware-in-the-wild-spreads-via-infected-office-documents/