PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
NoMachine Remote Privilege Escalation or DoS Vulnerability	NoMachine before 6.0.80 allows a remote attacker to gain privileges or cause a denial of service due to a flaw in the way parameters are handled in nxfs device drivers.	Version(s): <= 6.0.80	Published - February 21, 2018 CVE-2018-6947 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6947 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-6947
[cisco-sa-20180221-esc] Cisco Elastic Services Controller (ESC) Remote Code Execution Vulnerability - CVE-2018-0121	A vulnerability in the authentication functionality of the web-based service portal of Cisco Elastic Services Controller Software could allow an unauthenticated, remote attacker to bypass authentication and execute arbitrary actions with administrator privileges on an affected system. The vulnerability is due to improper security restrictions that are imposed by the web-based service portal of the affected software. An attacker could exploit this vulnerability by submitting an empty password value to an affected portal when prompted to enter an administrative password for the portal. A successful exploit could allow the attacker to bypass authentication and gain administrator privileges for the web-based service portal of the affected software. This vulnerability affects Cisco Elastic Services Controller Software Release 3.0.0. Cisco Bug IDs: CSCvg29809.	Version(s): <= 3.0.0	Published - February 21, 2018 CVE-2018-0121 CVSS - 9.8 Vendor's Advisory - http://www.securityfocus.com/bid/103113 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0121 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0121 http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180221-esc
Drupal 8.4.x before 8.4.5 Remote Information Disclosure and Content Modification	In Drupal versions 8.4.x versions before 8.4.5 users with permission to post comments are able to view content and comments they do not have access to, and are also able to add comments to this content. This vulnerability is mitigated by the fact that the comment system must be enabled and the attacker must have permission to post comments.	Version(s): <= 8.4.0 - 8.4.4	Published - February 21, 2018 CVE-2017-6926 CVSS - 9.1 Vendor's Advisory - http://www.securityfocus.com/bid/103115 https://qualysguard.qualys.com/fo/common/vuln_info.php?allow_modify=1&id=11933 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6926
Trend Micro Email Encryption Gateway <=5.5 Build 1111 Remote Command Execution Vulnerability via Log Hijacking - CVE-2018-6222	Trend Micro Email Encryption Gateway up to and including 5.5 Build 1111 is vulnerable to remote command execution via improper log file redirection and replacement. A remote attacker could configure full debug logs to be written to a selected location, and replace the directive with malicious code.	Version(s): = 5.5 Build 1111	Published - February 21, 2018 CVE-2018-6222 CVSS - 9.6 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6222 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-6222 https://success.trendmicro.com/solution/1119349-security-bulletin-trend-micro-email-encryption-gateway-5-5-multiple-vulnerabilities
Juniper AppFormix Remote Command Execution Vulnerability	A malicious user with unrestricted access to the AppFormix application management platform may be able to access a Python debug console and execute system commands with root privilege. The AppFormix Agent exposes the debug console on a host where AppFormix Agent is executing. If the host is executing AppFormix Agent, an attacker may access the debug console and execute Python commands with root privilege. Affected AppFormix releases are: all versions of 2.7; 2.11 versions prior to 2.11.3; 2.15 versions prior to 2.15.2. Juniper SIRT is not aware of any malicious exploitation of this vulnerability, however, the issue has been seen in a production network. No other Juniper Networks products or platforms are affected by this issue.	Version(s): <= 2.7.*, 2.11 - 2.11.2, 2.15 - 2.15.1	Published - February 22, 2018 CVE-2018-0015 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0015 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0015 https://kb.juniper.net/JSA10843
Siemens SIMATIC WinCC Add-Ons Remote Code Execution Vulnerability in Gemalto Sentinel Language Packs - CVE-2017-12819	Gemalto Sentinel LDK RTE, as used in multiple Siemens SIMATIC WinCC add-ons, is vulnerable to remote manipulations with language pack updater in an NTLM relay attack.	Version(s): <= 8	Published - February 22, 2018 CVE-2017-12819 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-12819 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-12819 https://cert-portal.siemens.com/productcert/pdf/ssa-127490.pdf
Citrix NetScaler ADC and NetScaler Gateway Remote Privilege Escalation Vulnerability - CVE-2018-6809	Citrix NetScaler ADC and NetScaler Gateway 10.5 - 10.5 Build 67.09, 11.0 - 11.0 Build 71.17, 11.1 - 11.1 Build 56.14, and 12.0 - 12.0 Build 57.18 are vulnerable to privilege escalation.	Version(s): <= 10.5 - 10.5 Build 67.09, 11.0 - 11.0 Build 71.17, 11.1 - 11.1 Build 56.14, 12.0 -12.0 Build 57.18	Published - March 01, 2018 CVE-2018-6809 CVSS - 9.8 Vendor's Advisory - https://qualysguard.qualys.com/fo/common/vuln_info.php?allow_modify=1&id=370797 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6809 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-6809
PHP Remote Stack Buffer Overflow Vulnerability	In PHP through 5.6.33, 7.0.x before 7.0.28, 7.1.x through 7.1.14, and 7.2.x through 7.2.2, there is a stack-based buffer under-read while parsing an HTTP response in the php_stream_url_wrap_http_ex function in ext/standard/http_fopen_wrapper.c. This subsequently results in copying a large string.	Version(s): <= 7.1 - 7.1.14, < 5.6.34, 7.0 - 7.0.27, 7.2 - 7.2.2	Published - March 01, 2018 CVE-2018-7584 CVSS - 9.8 Vendor's Advisory - http://www.securityfocus.com/bid/103204 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7584 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-7584
Postgresql Remote Code Execution Vulnerability	A flaw was found in the way Postgresql allowed a user to modify the behavior of a query for other users. An attacker with a user account could use this flaw to execute code with the permissions of superuser in the database. Versions 9.3 through 10 are affected.	Version(s): <= 9.3 - 9.3.21, 9.4 - 9.4.16, 9.6 - 9.6.7, 9.5 - 9.5.11, 10.2.*, 10 - 10.2	Published - March 02, 2018 CVE-2018-1058 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1058 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1058 https://bugzilla.redhat.com/show_bug.cgi?id=1547044
iThemes Security Plugin for WordPress <6.9.1 Unspecified Vulnerability	The iThemes Security plugin before 6.9.1 for WordPress does not properly perform data escaping for the logs page.	Version(s): <= 6.9.1	Published - March 02, 2018 CVE-2018-7433 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7433 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-7433
Wireshark 2.4.0 - 2.4.4 and 2.2.0 - 2.2.12 Remote DoS via a Crafted Package - CVE-2018-7331	In Wireshark 2.4.0 to 2.4.4 and 2.2.0 to 2.2.12, epan/dissectors/packet-ber.c had an infinite loop that was addressed by validating a length.	Version(s): <= 2.4.0 - 2.4.4, 2.2.0 - 2.2.12	Published - February 23, 2018 CVE-2018-7331 CVSS - 7.5 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7331 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-7331 https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=14444