PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
Apache Traffic Server HTTP Smuggling and Cache Poisoning - CVE-2018-8004	There are multiple HTTP smuggling and cache poisoning issues when clients making malicious requests interact with Apache Traffic Server (ATS). This affects versions 6.0.0 to 6.2.2 and 7.0.0 to 7.1.3. To resolve this issue users running 6.x should upgrade to 6.2.3 or later versions and 7.x users should upgrade to 7.1.4 or later versions.	Version(s): <= 7.0.0 - 7.1.3, 6.0.0 - 6.2.2	Published - August 30, 2018 CVE-2018-8004 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8004 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8004
Apache Traffic Server DoS Vulnerability - CVE-2018-8005	When there are multiple ranges in a range request, Apache Traffic Server (ATS) will read the entire object from cache. This can cause performance problems with large objects in cache. This affects versions 6.0.0 to 6.2.2 and 7.0.0 to 7.1.3. To resolve this issue users running 6.x users should upgrade to 6.2.3 or later versions and 7.x users should upgrade to 7.1.4 or later versions.	Version(s): <= 7.0.0 - 7.1.3, 6.0.0 - 6.2.2	Published - Aug 29, 2018 CVE-2018-8005 CVSS - 7.5 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8005 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8005
Apache Traffic Server Segmentation Fault Vulnerability - CVE-2018-8022	A carefully crafted invalid TLS handshake can cause Apache Traffic Server (ATS) to segfault. This affects version 6.2.2. To resolve this issue users running 6.2.2 should upgrade to 6.2.3 or later versions.	Version(s): <= 6.2.2	Published - Aug 29, 2018 CVE-2018-8022 CVSS - 7.5 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8022 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8022
Apache Traffic Server Segmentation Fault Vulnerability - CVE-2018-1318	Adding method ACLs in remap.config can cause a segfault when the user makes a carefully crafted request. This affects versions Apache Traffic Server (ATS) 6.0.0 to 6.2.2 and 7.0.0 to 7.1.3. To resolve this issue users running 6.x should upgrade to 6.2.3 or later versions and 7.x users should upgrade to 7.1.4 or later versions.	Version(s): <= 7.0.0 - 7.1.3, 6.0.0 - 6.2.2	Published - Aug 29, 2018 CVE-2018-1318 CVSS - 6.5 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1318 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1318
Linux Kernel Local DoS or Escalation of Privileges - CVE-2018-14619	A flaw was found in the crypto subsystem of the Linux kernel before version kernel-4.15-rc4. The "null skcipher" was being dropped when each af_alg_ctx was freed instead of when the aead_tfm was freed. This can cause the null skcipher to be freed while it is still in use leading to a local user being able to crash the system or possibly escalate privileges.	Version(s): < 4.14.8	Published - Aug 30, 2018 CVE-2018-14619 CVSS - 8.4 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-14619 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-14619
postgresql-jdbc <42.2.5 Remote Security Restrictions Bypass Vulnerability - CVE-2018-10936	A weakness was found in postgresql-jdbc before version 42.2.5. It was possible to provide an SSL Factory and not check the host name if a host name verifier was not provided to the driver. This could lead to a condition where a man-in-the-middle attacker could masquerade as a trusted server by providing a certificate for the wrong host, as long as it was signed by a trusted CA.	Version(s): < 42.2.5	Published - Aug 30, 2018 CVE-2018-10936 CVSS - 5.3 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10936 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-10936
IBM UrbanCode Deploy Remote Information Disclosure Vulnerability - CVE-2016-0373	IBM UrbanCode Deploy 6.0 through 6.2.2.1 could allow an authenticated user to read sensitive information due to UCD REST endpoints not properly authorizing users when determining who can read data. IBM X-Force ID: 112119.	Version(s): 6.0 - 6.2.2.1	Published - Aug 30, 2018 CVE-2018-0373 CVSS - 3.1 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0373 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0373
Wireshark 2.6.0 Remote DoS Vulnerability in Bluetooth AVDTP Dissector - CVE-2018-16058	In Wireshark 2.6.0 to 2.6.2, 2.4.0 to 2.4.8, and 2.2.0 to 2.2.16, the Bluetooth AVDTP dissector could crash. This was addressed in epan/dissectors/packet-btavdtp.c by properly initializing a data structure.	Version(s): = 2.2.0 - 2.2.16, 2.6.0 - 2.6.2, 2.4.0 - 2.4.8	Published - Aug 30, 2018 CVE-2018-16058 CVSS - 7.5 Vendor's Advisory - http://www.securityfocus.com/bid/105174 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-16058
Linux kernel <4.17.7 Remote Escalation of Privilege or DOS Vulnerability - CVE-2018-16276	An issue was discovered in yurex_read in drivers/usb/misc/yurex.c in the Linux kernel before 4.17.7. Local attackers could use user access read/writes with incorrect bounds checking in the yurex USB driver to crash the kernel or potentially escalate privileges.	Version(s): < 4.17.7	Published - Aug 31, 2018 CVE-2018-89788 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-16276 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-16276
[alert-cve-2018-11776-5072787-Third-Party-Component] Multiple Oracle Products Remote Code Execution in Apache Struts 2 - CVE-2018-11776	Apache Struts 2, as used in several Oracle products, could suffer from remote code execution when using results with no namespace and also the upper action(s) have no or wildcard namespace. The issue is also relevant when using a url tag which doesn't have a value and action set and also its upper action(s) have no or wildcard namespace. Oracle are currently investigating this issue. This record would be updated when detailed information of vulnerable products and available fixes is published by the vendor.	Version(s): 2.5 - 2.5.16, 2.3 - 2.3.34	Published - Aug 31, 2018 CVE-2018-11776 CVSS - 9.8 Vendor's Advisory - http://www.securityfocus.com/bid/105125 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11776