PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
TP-Link Router Remote Code Execution Vulnerability - CVE-2018-12577	TP-Link TL-WR841N V13 Router is prone to remote code injection vulnerability. An attacker can use the fact that ping and traceroute commands accept non-sanitated user input to perform OS command injection by sending specially crafted HTTP requests to the vulnerable router.	Version(s): <= WR841N V13	Published - July 01, 2018 CVE-2018-12577 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12577 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-12577
Google Android Remote Privilege Elevation Vulnerability in Kernel Components - CVE-2018-5703	The tcp_v6_syn_recv_sock function in net/ipv6/tcp_ipv6.c in the Linux kernel through 4.14.11 as used in Google Android 8.1 and earlier, before 2018-07-05 allows attackers to cause a denial of service (slab out-of-bounds write) or possibly have unspecified other impact via vectors involving TLS.	Version(s): <= 8.1	Published - July 02, 2018 CVE-2017-5703 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5703 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-5703
RedHat OpenShift Remote Code Execution Vulnerability via io.openshift.s2i.assemble-user Label - CVE-2018-10843	The source-to-image component of Openshift Container Platform before versions atomic-openshift 3.7.53 and atomic-openshift 3.9.31 is vulnerable to a privilege escalation which allows the assemble script to run as the root user in a non-privileged container. An attacker can use this flaw to open network connections, and possibly other actions, on the host which are normally only available to a root user.	Version(s): <= 3.7.53, 3.9 - 3.9.30	Published - July 02, 2018 CVE-2018-10843 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10843 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-10843
Siemens SICLOCK TC Remote DoS Vulnerability via NTP - CVE-2018-4851	A vulnerability has been identified in SICLOCK TC100 (All versions) and SICLOCK TC400 (All versions). An attacker with network access to the device could cause a Denial-of-Service condition by sending certain packets to the device, causing potential reboots of the device. The core functionality of the device could be impacted. The time serving functionality recovers when time synchronization with GPS devices or other NTP servers are completed.	Version(s): <= *	Published - July 03, 2018 CVE-2018-4851 CVSS - 9.1 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4851 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-4851
Ansible Remote Code Execution Vulnerability via Inventory Variables - CVE-2018-10874	Ansible is vulnerable to remote code execution due to inventory variables being loaded from the current working directory when running ad-hoc commands which are under attacker's control.	Version(s): <= *	Published - July 02, 2018 CVE-2018-10874 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10874 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-10874
Linux kernel <=4.17.3 Remote Unspecified Vulnerability - CVE-2018-13093	An issue was discovered in fs/xfs/xfs_icache.c in the Linux kernel through 4.17.3. There is a NULL pointer dereference and panic in lookup_slow() on a NULL inode->i_ops pointer when doing pathwalks on a corrupted xfs image. This occurs because of a lack of proper validation that cached inodes are free during allocation.	Version(s): <= 4.17.3	Published - July 03, 2018 CVE-2018-13093 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13093 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-13093 https://bugzilla.kernel.org/show_bug.cgi?id=199367
[MS18-JUL] Microsoft PowerShell Editor Services Remote Code Execution Vulnerability - CVE-2018-8327	Microsoft PowerShell Editor Services and PowerShell Extension for Visual Studio Code are prone to a remote code execution vulnerability.	Version(s): <= *	Published - July 10, 2018 CVE-2018-8327 CVSS - 9.8 Vendor's Advisory - http://www.securityfocus.com/bid/104649 https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2018-8327 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8327
SAP BusinessObjects and Crystal Reports Remote Code Execution Vulnerability - CVE-2018-2427	SAP BusinessObjects Business Intelligence Suite, versions 4.10 and 4.20, and SAP Crystal Reports (version for Visual Studio .NET, Version 2010) allows an attacker to inject code that can be executed by the application. An attacker could thereby control the behaviour of the application.	Version(s): <= 4.20, 4.10	Published - July 10, 2018 CVE-2018-2427 CVSS - 9.6 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-2427 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-2427
[APSB18-22] Adobe Connect Remote Privilege Escalation Vulnerability - CVE-2018-12805	Adobe Connect 9.7.5 and earlier is prone to privilege escalation vulnerability due to insecure library loading issue.	Version(s): <= 9.7.5	Published - July 11, 2018 CVE-2018-12805 CVSS - 9.8 Vendor's Advisory - http://www.securityfocus.com/bid/104696 https://qualysguard.qualys.com/fo/common/vuln_info.php?allow_modify=1&id=13194 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12805
Ansible 2 - 2.5, 2.6* Remote Code Execution Vulnerability - CVE-2018-10875	A flaw was found in ansible. ansible.cfg is read from the current working directory which can be altered to make it point to a plugin or a module path under the control of an attacker, thus allowing the attacker to execute arbitrary code.	Version(s): <= 2 - 2.5, 2.6*	Published - July 13, 2018 CVE-2018-10875 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10875 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-10875 https://www.ansible.com/