| PRODUCT | DESCRIPTION | AFFECTED VERSIONS | OTHER INFORMATION |
|---|---|---|---|
| Cisco IOS-XE Remote Authentication Bypass Vulnerability - CVE-2019-12643 | A vulnerability in the Cisco REST API virtual service container for Cisco IOS XE Software could allow an unauthenticated, remote attacker to bypass authentication on the managed Cisco IOS XE device. The vulnerability is due to an improper check performed by the area of code that manages the REST API authentication service. An attacker could exploit this vulnerability by submitting malicious HTTP requests to the targeted device. A successful exploit could allow the attacker to obtain the token-id of an authenticated user. This token-id could be used to bypass authentication and execute privileged actions through the interface of the REST API virtual service container on the affected Cisco IOS XE device. The REST API interface is not enabled by default and must be installed and activated separately on IOS XE devices. | 1.4.1, 1.5.1 ,1.6.1 ,1.7.1, 1.7.2, 1.8.1, 162.1, 99.99.99, 03.16.03, 03.16.04, 1.0.0, 1.2.1, 1.3.1, 1.4.1, 1.5.1, 1.6.1, 1.7.1, 1.8.1, 99.99.99, 2017.6, 2017.10, 162.1, 163.1 | Vendor - Cisco<br>CVE Id - CVE-2019-12643<br>CVSS Base - 10.0<br>Reporting Date - 08/28/2019<br>Vendor's Advisory - http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190828-iosxe-rest-auth-bypass |
| OpenStack os-vif Remote DoS or Information Disclosure Vulnerability in impl_pyroute2.py - CVE-2019-15753 | In OpenStack os-vif 1.15.x before 1.15.2, and 1.16.0, a hard-coded MAC aging time of 0 disables MAC learning in linuxbridge, forcing obligatory Ethernet flooding of non-local destinations, which both impedes network performance and allows users to possibly view the content of packets for instances belonging to other tenants sharing the same network. Only deployments using the linuxbridge backend are affected. This occurs in PyRoute2.add() in internal/command/ip/linux/impl_pyroute2.py. | 1.15 - 1.15.1, 1.16.0 | Vendor - Cisco<br>CVE Id - CVE-2019-15753<br>CVSS Base - 9.1<br>Reporting Date - 08/28/2019<br>Vendor's Advisory - https://security.openstack.org/ossa/OSSA-2019-004.html |
| Asus Precision TouchPad 11.0.0.25 Remote DoS or Privilege Escalation Vulnerability - CVE-2019-10709 | Asus Precision TouchPad version 11.0.0.25 suffers from denial of service and privilege escalation via pool overflow vulnerabilities. | 11.0.0.25 | Vendor - ASUS<br>CVE Id - CVE-2019-10709<br>CVSS Base - 9.8<br>Reporting Date - 08/30/2019<br>Vendor's Advisory - https://www.exploit-db.com/exploits/47322?utm_source=dlvr.it&utm_medium=twitter |
| GNU GLibC Remote Unspecified Vulnerability due to Insufficient Randomness in DARN - CVE-2019-15847 | The POWER9 backend in GNU Compiler Collection (GCC) before version 10 could optimize multiple calls of the __builtin_darn intrinsic into a single call, thus reducing the entropy of the random number generator. This occurred because a volatile operation was not specified. For example, within a single execution of a program, the output of every __builtin_darn() call may be the same. | <10 | Vendor - ASUS<br>CVE Id - CVE-2019-15847<br>CVSS Base - 7.5<br>Reporting Date - 09/02/2019<br>Vendor's Advisory - https://gcc.gnu.org/bugzilla/show_bug.cgi?id=91481 |
| Supermicro Servers Remote USB-based Attacks (USBAnywhere) | Authentication vulnerabilities in the baseboard management controllers (BMCs) of Supermicro X9-X11 servers have been discovered that allow a remote attacker to easily connect to a server and mount any virtual USB device of their choosing via the Virtual Media function ("USBAnywhere"). These vulnerabilities include plaintext authentication, weak encryption, and authentication bypass within the Virtual Media capabilities. | <1.71.5 | Vendor - Supermicro<br>CVE Id - CVE-2019-107043<br>CVSS Base - 9.8<br>Reporting Date - 09/03/2019<br>Vendor's Advisory - https://www.supermicro.com/support/security_BMC_virtual_media.cfm |
| Samba Share Path Escape Vulnerability Allows Remote Access to Unauthorized Directories - CVE-2019-10197 | A flaw was found in samba versions 4.9.x up to 4.9.13, samba 4.10.x up to 4.10.8 and samba 4.11.x up to 4.11.0rc3, when certain parameters were set in the samba configuration file. An unauthenticated attacker could use this flaw to escape the shared directory and access the contents of directories outside the share. | Samba 4.9 -4.9.12, 4.10 - 4.10.7, 4.11 - 4.11.0rc2<br>RedHat 7, 8 | Vendor - RedHat And Samba<br>CVE Id - CVE-2019-10297<br>CVSS Base - 9.1<br>Reporting Date - 09/03/2019<br>Vendor's Advisory - https://access.redhat.com/security/cve/cve-2019-10197 |
| Linux Kernel <=5.2.13 Remote Unspecified Vulnerability - CVE-2019-16089 | An issue was discovered in the Linux kernel through 5.2.13. nbd_genl_status in drivers/block/nbd.c does not check the nla_nest_start_noflag return value. | <=5.2.13 | Vendor - Linux<br>CVE Id - CVE-2019-16089<br>CVSS Base - 9.8<br>Reporting Date - 09/06/2019<br>Vendor's Advisory - https://lore.kernel.org/patchwork/patch/1106884/ |
| Linux kernel <5.2.3 Out of Bounds Access Vulnerability - CVE-2019-15926 | An issue was discovered in the Linux kernel before 5.2.3. Out of bounds access exists in the functions ath6kl_wmi_pstream_timeout_event_rx and ath6kl_wmi_cac_event_rx in the file drivers/net/wireless/ath/ath6kl/wmi.c. | <5.2.3 | Vendor - Linux<br>CVE Id - CVE-2019-15926<br>CVSS Base - 9.1<br>Reporting Date - 09/04/2019<br>Vendor's Advisory - https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.2.3 |
| Linux Kernel Remote Unspecified Vulnerability - CVE-2019-15902 | A backporting error was discovered in the Linux stable/longterm kernel 4.4.x through 4.4.190, 4.9.x through 4.9.190, 4.14.x through 4.14.141, 4.19.x through 4.19.69, and 5.2.x through 5.2.11. Misuse of the upstream "x86/ptrace: Fix possible spectre-v1 in ptrace_get_debugreg()" commit reintroduced the Spectre vulnerability that it aimed to eliminate. This occurred because the backport process depends on cherry picking specific commits, and because two (correctly ordered) code lines were swapped. | 4.19 - 4.19.69, 4.4 - 4.4.190, 1.14 - 4.14.141, 5.2 - 5.2.11, 4.9 - 4.9.190 | Vendor - Linux<br>CVE Id - CVE-2019-15902<br>CVSS Base - 9.8<br>Reporting Date - 09/04/2019<br>Vendor's Advisory - https://grsecurity.net/teardown_of_a_failed_linux_lts_spectre_fix.php |
| Cisco Content Security Management Virtual Appliance M600V HTTP Request Smuggling Attack | The Cisco Content Security Management Virtual Appliance M600V is prone to an http request smuggling attack which enables an attacker to poison one page with the contents of another page. | M600 | Vendor - Cisco<br>CVE Id - SBV-107140<br>CVSS Base - 9.8<br>Reporting Date - 09/04/2019<br>Vendor's Advisory - https://packetstormsecurity.com/files/154352 |