PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
Linux Kernel <2.6.20 Unspecified Vulnerability - CVE-2007-6762	In the Linux kernel before 2.6.20, there is an off-by-one bug in net/netlabel/netlabel_cipso_v4.c where it is possible to overflow the doi_def->tags[] array.	<2.6.20	Vendor - Linux CVE Id - CVE-2017-6762 CVSS Base - 9.8 Reporting Date - 07/27/2019 Vendor's Advisory - https://github.com/torvalds/linux/commit/2a2f11c227bdf292b3a2900ad04139d301b56ac4
Linux Kernel <2.6.34 Buffer Overflow Vulnerability - CVE-2010-5331	In the Linux kernel before 2.6.34, a range check issue in drivers/gpu/drm/radeon/atombios.c could cause an off by one (buffer overflow) problem	<2.6.34	Vendor - Linux CVE Id - CVE-2017-5331 CVSS Base - 9.8 Reporting Date - 07/27/2019 Vendor's Advisory - https://github.com/torvalds/linux/commit/2a2f11c227bdf292b3a2900ad04139d301b56ac4
Linux Kernel <2.6.37 Out of Array Bounds Access Unspecified Vulnerability - CVE-2010-5332	In the Linux kernel before 2.6.37, an out of bounds array access happened in drivers/net/mlx4/port.c. When searching for a free entry in either mlx4_register_vlan() or mlx4_register_mac(), and there is no free entry, the loop terminates without updating the local variable free thus causing out of array bounds access.	<2.6.37	Vendor - Linux CVE Id - CVE-2017-5332 CVSS Base - 9.8 Reporting Date - 07/27/2019 Vendor's Advisory - https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=0926f91083f34d047abc74f1ca4fa6a9c161f7db
Linux Kernel <3.1 Memory Corruption Vulnerability - CVE-2011-5327	In the Linux kernel before 3.1, an off by one in the drivers/target/loopback/tcm_loop.c tcm_loop_make_naa_tpg() function could result in at least memory corruption.	<3.1	Vendor - Linux CVE Id - CVE-2017-5327 CVSS Base - 9.8 Reporting Date - 07/27/2019 Vendor's Advisory - https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=12f09ccb4612734a53e47ed5302e0479c10a50f8
Linux Kernel <4.16.4 Remote Unspecified Vulnerability due to Deadlock - CVE-2019-14763	In the Linux kernel before 4.16.4, a double-locking error in drivers/usb/dwc3/gadget.c may potentially cause a deadlock with f_hid.	<4.16.4	Vendor - Linux CVE Id - CVE-2019-14763 CVSS Base - 9.8 Reporting Date - 08/07/2019 Vendor's Advisory - https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=072684e8c58d17e853f8e8b9f6d9ce2e58d2b036
Linux Kernel <4.16.4 Remote DoS or Other Vulnerability in f_midi Driver - CVE-2018-20961	In the Linux kernel before 4.16.4, a double free vulnerability in the f_midi_set_alt function of drivers/usb/gadget/function/f_midi.c in the f_midi driver may allow attackers to cause a denial of service or possibly have unspecified other impact.	<4.16.4	Vendor - Linux CVE Id - CVE-2019-20961 CVSS Base - 9.8 Reporting Date - 08/07/2019 Vendor's Advisory - https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=7fafcfdf6377b18b2a726ea554d6e593ba44349f
Cisco Small Business 220 Series Smart Plus Switches Remote Authentication Bypass Vulnerability - CVE-2019-1912	A vulnerability in the web management interface of Cisco Small Business 220 Series Smart Switches could allow an unauthenticated, remote attacker to upload arbitrary files. The vulnerability is due to incomplete authorization checks in the web management interface. An attacker could exploit this vulnerability by sending a malicious request to certain parts of the web management interface. Depending on the configuration of the affected switch, the malicious request must be sent via HTTP or HTTPS. A successful exploit could allow the attacker to modify the configuration of an affected device or to inject a reverse shell. This vulnerability affects Cisco Small Business 220 Series Smart Switches running firmware versions prior to 1.1.4.4 with the web management interface enabled. The web management interface is enabled via both HTTP and HTTPS by default.	<1.1.4.4	Vendor - Cisco CVE Id - CVE-2019-1912 CVSS Base - 9.1 Reporting Date - 08/06/2019 Vendor's Advisory - http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190806-sb220-auth_bypass
Cisco Small Business 220 Series Smart Plus Switches Remote Code Execution Vulnerability - CVE-2019-1913	Multiple vulnerabilities in the web management interface of Cisco Small Business 220 Series Smart Switches could allow an unauthenticated, remote attacker to overflow a buffer, which then allows the execution of arbitrary code with root privileges on the underlying operating system. The vulnerabilities are due to insufficient validation of user-supplied input and improper boundary checks when reading data into an internal buffer. An attacker could exploit these vulnerabilities by sending malicious requests to the web management interface of an affected device. Depending on the configuration of the affected switch, the malicious requests must be sent via HTTP or HTTPS.	<1.1.4.4	Vendor - Cisco CVE Id - CVE-2019-1913 CVSS Base - 9.8 Reporting Date - 08/06/2019 Vendor's Advisory - http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190806-sb220-rce
Google Android Code Execution Vulnerability in Broadcom Components - CVE-2019-11516	Google Android up to and including version 9 before 2019-08-05 is vulnerable to a critical severity code execution vulnerability in broadcom components. AKA Android Bug ID A-132966035.	<=9	Vendor - Google CVE Id - CVE-2019-11516 CVSS Base - 9.8 Reporting Date - 08/05/2019 Vendor's Advisory - https://source.android.com/security/bulletin/2019-08-01
Google Android Remote Code Execution Vulnerability in Qualcomm Components - CVE-2019-10538	Google Android up to and including version 9 before 2019-08-05 is vulnerable to a high severity vulnerability in the qualcomm Wi-Fi controller. The vulnerability enables malicious code running within the Wi-Fi controller to overwrite parts of the Linux kernel running the main Android operating system, and subsequently fully compromise the device. AKA Android Bug ID A-132193791. NOTE: The 2019-08-01 patch level applies to Pixel devices only.	<=9	Vendor - Google CVE Id - CVE-2019-10538 CVSS Base - 9.8 Reporting Date - 08/05/2019 Vendor's Advisory - https://source.android.com/security/bulletin/2019-08-01
Google Android Buffer Overflow Vulnerability in Qualcomm Closed-source Components - CVE-2019-10539, CVE-2019-10540	Google Android up to and including version 9 before 2019-08-05 is vulnerable to a critical severity vulnerability in qualcomm closed-source components. The vulnerability is due to a buffer overflow issue in the Qualcomm WLAN firmware because of inadequate checks when parsing the extended cap IE header length. AKA Android Bug ID A-135126805. NOTE: The 2019-08-01 patch level applies to Pixel devices only.	<=9	Vendor - Google CVE Id - CVE-2019-10540, CVE-2019-10539 CVSS Base - 9.8 Reporting Date - 08/05/2019 Vendor's Advisory - https://source.android.com/security/bulletin/2019-08-01
Symantec Endpoint Protection Local Privilege Escalation Vulnerability - CVE-2019-12750	Symantec Endpoint Protection, prior to 14.2 RU1 & 12.1 RU6 MP10 and Symantec Endpoint Protection Small Business Edition, prior to 12.1 RU6 MP10c (12.1.7491.7002), may be susceptible to a privilege escalation vulnerability, which is a type of issue whereby an attacker may attempt to compromise the software application to gain elevated access to resources that are normally protected from an application or user.	Endpoint Protection 14 - 14.2 RUO, <12.1 RUG MP10 Endpoint Protection small Bussiness Enterprise<12.1 RUG MP10c (12.1.7491.7002)	Vendor -Symantec CVE Id - CVE-2019-12750 CVSS Base - 8.4 Reporting Date - 07/31/2019 Vendor's Advisory - https://support.symantec.com/us/en/article.SYMSA1487.html
Cisco Nexus Local Network Code Execution Vulnerability via LLDP Frame Headers - CVE-2019-1901	A vulnerability in the Link Layer Discovery Protocol (LLDP) subsystem of Cisco Nexus 9000 Series Application Centric Infrastructure (ACI) Mode Switch Software could allow an adjacent, unauthenticated attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges. The vulnerability is due to improper input validation of certain type, length, value (TLV) fields of the LLDP frame header. An attacker could exploit this vulnerability by sending a crafted LLDP packet to the targeted device. A successful exploit may lead to a buffer overflow condition that could either cause a DoS condition or allow the attacker to execute arbitrary code with root privileges. Note: This vulnerability cannot be exploited by transit traffic through the device; the crafted packet must be targeted to a directly connected interface. This vulnerability affects Cisco Nexus 9000 Series Fabric Switches in ACI mode if they are running a Cisco Nexus 9000 Series ACI Mode Switch Software release prior to 13.2(7f) or any 14.x release.	Cisco Nexus 9000 Series ACI Mode Switch Software release prior to 13.2(7f) or any 14.x release	Vendor - Cisco CVE Id - CVE-2019-1901 CVSS Base - 8.8 Reporting Date - 07/31/2019 Vendor's Advisory - https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190731-nxos-bo

PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
Apple MacOS X Local Network MitM Vulnerability in AWDL	Apple MacOS X is vulnerable to man-in-the-middle attacks due to ambiguous receiver authentication state in Airdrop's implementation of Apple Wireless Direct Link (AWDL). Insufficient differentiation and controls in the GUI allows unauthenticated devices to connect in the guise of authenticated ones. This could enable an attacker to gain a man-in-the-middle position and modify or downgrade the device's firmware.	*	Vendor - Apple CVSS Base - 8.8 Reporting Date - 07/31/2019 Vendor's Advisory - https://www.helpnetsecurity.com/2019/07/31/apple-airdrop-issues/
Xerox Phaser Remote Code Execution or DoS Vulnerability in IPP - CVE-2019-13165, CVE-2019-13168	Xerox Phaser 3320 printers with firmware version 53.006.16.000 are vulnerable to remote code execution and denial of service. A remote attacker could send malicious requests to the IPP service to crash or execute code on an affected device.	53.006.16.00	Vendor - Xerox CVE Id - CVE-2019-13168, CVE-2019-13165 CVSS Base - 9.8 Reporting Date - 08/08/2019 Vendor's Advisory - https://www.nccgroup.trust/uk/our-research/technical-advisory-multiple-vulnerabilities-in-xerox-printers/
Xerox Phaser Remote Code Execution or DoS Vulnerability in Google Cloud Print - CVE-2019-13171, CVE-2019-13172, CVE-2019-13169,	Xerox Phaser 3320 printers with firmware version 53.006.16.000 are vulnerable to remote code execution and denial of service in their Google Cloud Print implementation. A remote attacker could modify register parameters to trigger a stack buffer overflow in memcpy().	53.006.16.00	Vendor - Xerox CVE Id - CVE-2019-13171, CVE-2019-13172, CVE-2019-13169, CVSS Base - 9.8 Reporting Date - 08/08/2019 Vendor's Advisory - https://www.nccgroup.trust/uk/our-research/technical-advisory-multiple-vulnerabilities-in-xerox-printers/
Huawei PCManager Remote Code Execution Vulnerability - CVE-2019-5238	Huawei PCManager with the versions before 9.0.1.66 (Oversea) and versions before 9.0.1.70 (China) have a code execution vulnerability. Successful exploitation may cause the attacker to execute code and read/write information.	<9.0.1.70 China, <9.0.1.66 Oversea	Vendor - Huawei CVE Id - CVE-2019-5238, CVE-2019-5237, CVSS Base - 7.8 Reporting Date - 08/08/2019 Vendor's Advisory - https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20190710-01-pcmanager-en