Common Vulnerabilities and Exposures (CVE) Addressed in Open Source Components in Cisco IOS XE Bengaluru 17.6.1

Revised: August 10, 2021

Common Vulnerabilities and Exposures Addressed in Open Source Components in Cisco IOS XE Bengaluru 17.6.x

Information About Common Vulnerabilities and Exposures

This document contains information about patched Common Vulnerabilities and Exposures (CVE) for open source software (OSS) used in this product. The updating of an OSS component does not necessarily imply that IOS XE itself was previously vulnerable. This is done to improve the general security posture of the product. The CVE ID in the following table links to the corresponding vulnerability entry on the National Vulnerability Database (NVD). To view the details of a vulnerability, click on the CVE ID.

Note This Cisco product may contain third-party software that includes open source components (including those listed below) with unpatched vulnerabilities. Many of these vulnerabilities do not have a known attack vector.

To learn about Cisco security vulnerability disclosure policies and publications, see the Security Vulnerability Policy. The policy also contains instructions for obtaining fixed software and receiving security vulnerability information from Cisco.

Licensing information about the open source software used in this product can be found at Open Source Notices & Documentation. With respect to the open source software listed in this document, if you have any questions or wish to receive a copy of any source code to which you may be entitled under the applicable open source license(s) (such as the GNU Lesser/General Public License), contact us at external-opensource-requests@cisco.com.

Common Vulnerabilities and Exposures (CVE) Addressed in Open Source Components in Cisco IOS XE Bengaluru 17.6.1

CVE ID	Component	Component Version
CVE-2017-6519	avahi	0.7
CVE-2012-3410 CVE-2014-6271 CVE-2014-6277 CVE-2014-6278 CVE-2014-7169 CVE-2014-7186 CVE-2014-7187 CVE-2016-7543 CVE-2016-9401 CVE-2019-9924	bash	4.2

CVE ID	Component	Component Version
CVE-2020-8622 CVE-2020-8623 CVE-2020-8624	bind	9.11.19
CVE-2019-12972 CVE-2019-14250 CVE-2019-14444 CVE-2019-17450 CVE-2019-17451 CVE-2019-9070 CVE-2019-9071 CVE-2019-9074 CVE-2019-9075 CVE-2019-9076 CVE-2019-9077	binutils	2.32
CVE-2018-10910 CVE-2020-0556	bluez	5.5
CVE-2012-2677	boost	1.71.0
CVE-2017-7475 CVE-2018-19876 CVE-2019-6461 CVE-2019-6462	cairo	1.16.0
CVE-2020-1971 CVE-2021-3449	ciscossl	1.1.1c.7.1.3
CVE-2019-11834 CVE-2019-11835	cjson	1.7.10+gitAUTOINC+c69134d017
CVE-2015-1197 CVE-2016-2037 CVE-2019-14866	cpio	2.12
CVE-2016-6318	cracklib	2.9.5
CVE-2019-15601	curl	7.66.0
CVE-2020-12049	dbus	1.12.16

CVE ID	Component	Component Version
CVE-2019-18218	file	5.37
CVE-2016-6354	flex	2.6.0
CVE-2019-14250 CVE-2019-15847	gcc	9.2.0
CVE-2019-1010180	gdb	8.3.1
CVE-2018-18751	gettext	0.19.8.1
CVE-2020-6750	glib	2.60.7
CVE-2019-19126 CVE-2020-10029 CVE-2020-1751 CVE-2020-1752 CVE-2020-6096	glibc	2.3
CVE-2020-13777 CVE-2020-24659	gnutls	3.6.13
CVE-2020-10531	international_components_for_unicode	64.2
CVE-2020-12762	json-c	0.13.1
CVE-2019-19221 CVE-2020-9308	libarchive	3.4.0
CVE-2018-14348	libcgroup	0.41
CVE-2019-15601	libcurl	7.66.0
CVE-2019-12904 CVE-2019-13627	libgcrypt	1.8.4
CVE-2019-19956 CVE-2019-20388 CVE-2020-7595	libxml2	2.9.9
CVE-2019-11068 CVE-2019-13117 CVE-2019-13118 CVE-2019-18197	libxslt	1.1.33
CVE-2018-10195	lrzsz	0.12.20

CVE ID	Component	Component Version
CVE-2004-2771 CVE-2014-7844	mailx	12.5-5
CVE-2019-17594 CVE-2019-17595	ncurses	6.1.20190803
CVE-2019-7282 CVE-2019-7283	netkit-rsh	0.17
CVE-2020-10188	netkit-telnet	0.17
CVE-2020-11080	nghttp2	1.39.2
CVE-2019-16905	openssh	8.0p1
CVE-2020-14155	pcre	8.43
CVE-2020-10543 CVE-2020-10878	perl	5.30.1
CVE-2015-3310 CVE-2020-8597	ppp	2.4.7
CVE-2019-9674	python	2.7.18
CVE-2020-14422	python	3.7.8
CVE-2013-7459	python3-pycrypto	2.6.1
CVE-2013-7459	python-pycrypto	2.6.1

CVE ID	Component	Component Version
CVE-2019-12068 CVE-2019-15890 CVE-2019-20382 CVE-2020-10702 CVE-2020-10756 CVE-2020-11869 CVE-2020-13765 CVE-2020-14364 CVE-2020-15863 CVE-2020-16092 CVE-2020-1711 CVE-2020-7039 CVE-2020-7211	qemu	4.1.0
CVE-2016-9840 CVE-2016-9841 CVE-2016-9842 CVE-2016-9843	rsync	3.1.3
CVE-2020-9366	screen	4.6.2
CVE-2019-16168 CVE-2019-19244 CVE-2019-19923 CVE-2019-19924 CVE-2019-19925 CVE-2019-19926 CVE-2019-19959 CVE-2019-20218 CVE-2020-11655	sqlite	3.29.0
CVE-2019-14287 CVE-2021-3156	sudo	1.8.27
CVE-2019-16167 CVE-2019-19725	sysstat	12.1.6

CVE ID	Component	Component Version
CVE-2020-13776 CVE-2020-1712	systemd	243.2
CVE-2014-8139 CVE-2014-8140 CVE-2014-8141 CVE-2014-9636 CVE-2014-9913 CVE-2015-1315 CVE-2015-7696 CVE-2015-7697 CVE-2016-9844 CVE-2018-1000035 CVE-2018-18384 CVE-2019-13232	unzip	6
CVE-2013-4342	xinetd	2.3.15

Additional Resources

Related Topic	Resource
Cisco Security Advisories	https://tools.cisco.com/security/center/publicationListing.x
Cisco Security Vulnerability Policy	http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html
Common Vulnerabilities and Exposures	https://cve.mitre.org/index.html
Open Source In Cisco Products	https://www.cisco.com/c/en/us/about/legal/open-source-documentation-responsive.html

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.