Common Vulnerabilities and Exposures (CVE) Addressed in Open Source Components in Cisco IOS XE Bengaluru 17.4.1

Revised: December 13, 2020

Common Vulnerabilities and Exposures Addressed in Open Source Components in Cisco IOS XE Bengaluru 17.4.1

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 Fixed in Open Source Components in Cisco IOS XE Bengaluru 17.4.1

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

CVE ID	Component	Component Version
CVE-2014-6271	bash	4.2
CVE-2019-12972	binutils	2.32
CVE-2019-14250	binutils	2.32
CVE-2019-14444	binutils	2.32
CVE-2019-9071	binutils	2.32
CVE-2019-9074	binutils	2.32
CVE-2019-9076	binutils	2.32
CVE-2019-17450	binutils	2.32
CVE-2019-17451	binutils	2.32
CVE-2019-9070	binutils	2.32
CVE-2019-9075	binutils	2.32
CVE-2019-9077	binutils	2.32
CVE-2020-0556	bluez	5.48
CVE-2018-19876	cairo	1.16.0
CVE-2019-6461	cairo	1.16.0
CVE-2019-6462	cairo	1.16.0
CVE-2019-11834	cjson	1.7.10+gitAUTOINC+c69134d017
CVE-2019-11835	cjson	1.7.10+gitAUTOINC+c69134d017
CVE-2019-14866	cpio	2.12
CVE-2020-12049	dbus	1.12.16
CVE-2019-14834	dnsmasq	2.80
CVE-2019-18218	file	5.37
CVE-2016-6354	flex	2.6.0
CVE-2019-15847	gcc	9.2.0
CVE-2020-6750	glib	2.60.7
CVE-2019-19126	glibc	2.30
CVE-2020-10029	glibc	2.30
CVE-2020-1751	glibc	2.30

CVE ID	Component	Component Version
CVE-2020-1752	glibc	2.30
CVE-2020-6096	glibc	2.30
CVE-2020-13777	gnutls	3.6.13
CVE-2020-10531	international_components_for_unicode	64.2
CVE-2020-12762	json-c	0.13.1
CVE-2019-19221	libarchive	3.4.0
CVE-2020-9308	libarchive	3.4.0
CVE-2018-14348	libcgroup	0.41
CVE-2019-12904	libgcrypt	1.8.4
CVE-2019-19956	libxml2	2.9.9
CVE-2019-13117	libxslt	1.1.33
CVE-2019-13118	libxslt	1.1.33
CVE-2019-11068	libxslt	1.1.33
CVE-2019-17594	ncurses	6.1.20190803
CVE-2019-17595	ncurses	6.1.20190803
CVE-2020-11080	nghttp2	1.39.2
CVE-2019-16905	openssh	8.0p1
CVE-2020-14155	pcre	8.43
CVE-2020-10543	perl	5.30.1
CVE-2020-10878	perl	5.30.1
CVE-2020-14422	python	3.7.8
CVE-2019-9674	python	2.7.18
CVE-2020-11869	qemu	4.1.0
CVE-2019-20382	qemu	4.1.0
CVE-2020-10702	qemu	4.1.0
CVE-2020-13765	qemu	4.1.0
CVE-2020-1711	qemu	4.1.0
CVE-2019-15890	qemu	4.1.0

CVE ID	Component	Component Version
CVE-2020-9366	screen	4.6.2
CVE-2019-16168	sqlite	3.29.0
CVE-2020-11655	sqlite	3.29.0
CVE-2019-14287	sudo	1.8.27
CVE-2019-19725	sysstat	12.1.6
CVE-2020-13776	systemd	243.2
CVE-2020-1712	systemd	243.2
CVE-2019-13232	unzip	6.0
CVE-2014-9913	unzip	6.0
CVE-2016-9844	unzip	6.0
CVE-2015-7697	unzip	6.0
CVE-2014-9636	unzip	6.0
CVE-2018-18384	unzip	6.0
CVE-2015-7696	unzip	6.0
CVE-2014-8139	unzip	6.0
CVE-2014-8140	unzip	6.0
CVE-2014-8141	unzip	6.0
CVE-2018-1000035	unzip	6.0

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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

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.