Cisco Security Advisory

Multiple Vulnerabilities in Cisco WebEx Recording Format and Advanced Recording Format Players

Advisory ID: cisco-sa-20171129-webex-players
Last Updated: 2017 November 30 23:36 GMT
Published: 2017 November 29 16:00 GMT
Version1.3: Final
CVSS Score: Base - 9.6
Workarounds: No workarounds available
Cisco Bug IDs: CSCve02843 CSCve10584 CSCve10591 CSCve10658 CSCve10744 CSCve10749 CSCve10762 CSCve10764 CSCve11503 CSCve11507 CSCve11532 CSCve11538 CSCve11545 CSCve11548 CSCve30208 CSCve30214 CSCve30268 CSCvf38060 CSCvf38077 CSCvf38084 CSCvf49650 CSCvf49697 CSCvf49707 CSCvf57234 CSCvg54836 CSCvg54843 CSCvg54850 CSCvg54853 CSCvg54856 CSCvg54861 CSCvg54867 CSCvg54868 CSCvg54870

CVE-2017-12367
CVE-2017-12368
CVE-2017-12369
CVE-2017-12370
CVE-2017-12371
CVE-2017-12372
CWE-119
CWE-125
CWE-20

Download CVRF
Download PDF
Email

Cisco Security Vulnerability Policy

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

Subscribe to Cisco Security Notifications

Subscribe

Summary

Multiple vulnerabilities exist in Cisco WebEx Network Recording Player for Advanced Recording Format (ARF) and WebEx Recording Format (WRF) files. A remote attacker could exploit these vulnerabilities by providing a user with a malicious ARF or WRF file via email or URL and convincing the user to launch the file. Exploitation of these vulnerabilities could cause an affected player to crash and, in some cases, could allow arbitrary code execution on the system of a targeted user.

The Cisco WebEx players are applications that are used to play back WebEx meeting recordings that have been recorded by an online meeting attendee. The player can be automatically installed when the user accesses a recording file that is hosted on a WebEx server.

Cisco has updated affected versions of the Cisco WebEx Business Suite meeting sites, Cisco WebEx Meetings sites, Cisco WebEx Meetings Server, and Cisco WebEx ARF and WRF Players to address these vulnerabilities. There are no workarounds that address these vulnerabilities.

This advisory is available at the following link:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171129-webex-players

Affected Products

Vulnerable Products

The vulnerabilities disclosed in this advisory affect the Cisco WebEx ARF Player and the Cisco WebEx WRF Player. The following client builds of Cisco WebEx Business Suite (WBS30, WBS 31, and WBS32), Cisco WebEx Meetings, and Cisco WebEx Meetings Server are affected by at least one of the vulnerabilities described in this advisory:

- Cisco WebEx Business Suite (WBS30) client builds prior to T30.20
- Cisco WebEx Business Suite (WBS31) client builds prior to T31.14.1
- Cisco WebEx Business Suite (WBS32) client builds prior to T32.2
- Cisco WebEx Meetings with client builds prior to T31.14
- Cisco WebEx Meeting Server builds prior to 2.7MR3

To determine whether a Cisco WebEx meeting site is running an affected version of the WebEx client build, users can log in to their Cisco WebEx meeting site and go to the **Support Downloads** section. The version of the WebEx client build will be displayed on the right side of the page under **About Meeting Center**. See the "Fixed Software" section for details.

Alternatively, version information of the Cisco WebEx meeting client can be accessed from within the Cisco WebEx meeting client. Version information for the Cisco WebEx meeting client on Windows and Linux platforms can be viewed by choosing **Help About Cisco WebEx Meeting Center**. Version information for the Cisco WebEx meeting client on Mac platforms can be viewed by choosing **Meeting Center About Cisco WebEx Meeting Center**.

The Cisco WebEx software updates are cumulative in client builds. For example, if client build 30.32.16 is fixed, build 30.32.17 will contain updated software. Cisco WebEx site administrators have access to secondary version nomenclature, for example, T30 SP32 EP 16, which shows that the server is running client build 30.32.16.

Note: Customers who do not receive automatic software updates may be running versions of Cisco WebEx that have reached end of software maintenance and should contact customer support.

Products Confirmed Not Vulnerable

No other Cisco products are currently known to be affected by these vulnerabilities.

Details

The Cisco WebEx Business Suite (WBS) meeting services and Cisco WebEx Meetings are a hosted multimedia conferencing solution that is managed and maintained by Cisco WebEx. The Cisco WebEx Meetings Server is a multimedia conferencing solution that customer can host in their private clouds.

The ARF and WRF file formats are used to store WebEx meeting recordings that have been recorded on a WebEx meeting site, or on the computer of an online meeting attendee.

The Cisco WebEx ARF Player and the Cisco WebEx WRF Player are applications that are used to play back and edit WebEx ARF and WRF recording files (files with .arf and .wrf extensions).

The Cisco WebEx ARF Player and Cisco WebEx WRF Player can be automatically installed when a user accesses a recording file that is hosted on a WebEx meeting site (for streaming playback mode). The Cisco WebEx ARF Player and Cisco WebEx WRF Player can also be manually installed after downloading the application from http://www.webex.com/play-webex-recording.html to play back recording files for offline playback.

The Cisco WebEx ARF Player is available for all Cisco WebEx meeting site clients (WBS30, WBS31, WBS32, and WebEx Meetings) and for Cisco WebEx Meetings Server clients. The Cisco WebEx WRF Player is only available for Cisco WebEx WBS30, WBS 31, and WBS32 meeting site clients and is not available for the Cisco WebEx Meetings or Cisco WebEx Meetings Server clients.

The following table provides the Cisco bug IDs and Common Vulnerabilities and Exposures (CVE) identifiers that have been assigned for the vulnerabilities in this advisory:

Title	CVE ID	Cisco Bug ID
Cisco WebEx Network Recording Player Denial of Service Vulnerability	CVE-2017-12367	CSCve11545, CSCve02843, CSCve11548
Cisco WebEx Network Recording Player Remote Code Execution Vulnerability	CVE-2017-12368	CSCve10584, CSCve10591, CSCve11503, CSCve10658, CSCve11507, CSCve10749, CSCve10744, CSCve11532, CSCve10762, CSCve10764, CSCve11538
Cisco WebEx Network Recording Player Out-of-Bounds Vulnerability	CVE-2017-12369	CSCve30208, CSCve30214, CSCve30268
Cisco WebEx Network Recording Player Remote Code Execution Vulnerability	CVE-2017-12370	CSCvf38060, CSCvg54836, CSCvf38077, CSCvg54843, CSCvf38084, CSCvg54850
Cisco WebEx Network Recording Player Remote Code Execution	CVE-2017-12371	CSCvf49650, CSCvg54853, CSCvg54856, CSCvf49697,

Vulnerability		**CSCvg54861, CSCvf49707, CSCvg54867**
Cisco WebEx Network Recording Player Remote Code Execution Vulnerability	**CVE-2017-12372**	**CSCvf57234, CSCvg54868, CSCvg54870**

Exploitation of these vulnerabilities may cause player applications to crash or, in some cases, execute malicious code from a remote attacker.

To exploit these vulnerabilities, the player application would need to open a malicious ARF or WRF file. An attacker may be able to accomplish this exploit by providing the malicious recording file directly to users (for example, by using email), or by directing a user to a malicious web page. The vulnerabilities cannot be triggered by users who are attending a WebEx meeting.

Workarounds

There are no workarounds that address these vulnerabilities. However, it is possible to remove all WebEx software completely from a system using the Meeting Services Removal Tool (for Microsoft Windows users) or Mac WebEx Meeting Application Uninstaller (for Apple Mac OS X users) available for download from the Cisco Collaboration Help for Cisco Spark, WebEx, and Jabber article at https://collaborationhelp.cisco.com/article/en-us/WBX000026396.

Removal of the WebEx software from a Linux or UNIX-based system can be accomplished by following the steps in the Cisco Collaboration Help for Cisco Spark, WebEx, and Jabber article: https://collaborationhelp.cisco.com/article/en-us/WBX28548.

Fixed Software

Cisco has released free software updates that address the vulnerability described in this advisory. Customers may only install and expect support for software versions and feature sets for which they have purchased a license. By installing, downloading, accessing, or otherwise using such software upgrades, customers agree to follow the terms of the Cisco software license: http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html

Additionally, customers may only download software for which they have a valid license, procured from Cisco directly, or through a Cisco authorized reseller or partner. In most cases this will be a maintenance upgrade to software that was previously purchased. Free security software updates do not entitle customers to a new software license, additional software feature sets, or major revision upgrades.

When considering software upgrades, customers are advised to regularly consult the advisories for Cisco products, which are available from the Cisco Security Advisories and Alerts page, to determine exposure and a complete upgrade solution.

In all cases, customers should ensure that the devices to upgrade contain sufficient memory and confirm that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, customers are advised to contact the Cisco Technical Assistance Center (TAC) or their contracted maintenance providers.

Customers Without Service Contracts

Customers who purchase directly from Cisco but do not hold a Cisco service contract and customers who make purchases through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should obtain upgrades by contacting the Cisco TAC:
http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

Customers should have the product serial number available and be prepared to provide the URL of this advisory as evidence of entitlement to a free upgrade.

Fixed Releases

The following client builds of Cisco WebEx Business Suite (WBS30, WBS31, WBS32), Cisco WebEx Meetings, and Cisco WebEx Meetings Server address all the vulnerabilities described in this advisory:

- Cisco WebEx Business Suite (WBS30) client builds T30.20 and later
- Cisco WebEx Business Suite (WBS31) client builds T31.20 and later
- Cisco WebEx Business Suite (WBS32) client builds T32.7 and later
- Cisco WebEx Meetings with client builds T32.7 and later
- Cisco WebEx Meeting Server builds 2.7MR3 and later, 2.8MR1 and later, 3.0 and later

To determine whether a Cisco WebEx meeting site is running an affected version of the WebEx client build, users can log in to their Cisco WebEx meeting site and go to the **Support Downloads** section. The version of the WebEx client build will be displayed on the right side of the page under **About Meeting Center**. The Cisco WebEx software updates are cumulative in client builds. For example, if client build 30.32.16 is fixed, build 30.32.17 will contain updated software.

The vulnerabilities disclosed in this advisory affect the Cisco WebEx ARF and WRF Players. The Microsoft Windows, Apple Mac OS X, and Linux versions of the players are all affected by at least one vulnerability described in this advisory. If the Cisco WebEx ARF Player or the Cisco WebEx WRF Player was automatically installed, it will be automatically upgraded to the latest, non-vulnerable version when users access a recording file that is hosted on a WebEx meeting site. If the Cisco WebEx ARF Player or the Cisco WebEx WRF Player was manually installed, users will need to manually install a new version of the player after downloading the latest version from http://www.webex.com/play-webex-recording.html.

Users can manually verify the installed version of the Cisco WebEx ARF Player or the Cisco WebEx WRF Player to determine whether they are affected by these vulnerabilities.

NOTE: Users whose WebEx Business Suites are on lockdown will need to contact WebEx Support to apply the appropriate patch to their WebEx site.

Cisco Bug ID	First Fixed Release				
	WBS30	WBS31	WBS32	WebEx Meetings	WebEx Meetings Server
CSCve11545					2.7MR3 2.8MR1
CSCve02843	T30.20	T31.14	T32.2		
CSCve11548				T30.20 T32.2	
CSCve10584		T31.14.4 T31.15	T32.3		
CSCve10591					2.7MR3 2.8MR1
CSCve11503				T32.3	
CSCve10658		T31.14.4	T32.4		
CSCve11507				T32.3	
CSCve10749					2.7MR3 2.8MR1
CSCve10744		T31.14.4	T32.2		
CSCve11532				T32.2	
CSCve10762			T32.4		
CSCve10764					3.0
CSCve11538				T32.2	
CSCve30208		T31.14.4 T31.15 T31.17.2	T32.3 T32.6		
CSCve30214					2.7MR3 2.8MR1
CSCve30268				T32.4 T32.6	
CSCvf38060		T31.17	T32.5		
CSCvg54836				T32.7	
CSCvf38077		T31.17	T32.5		
CSCvg54843				T32.7	
CSCvf38084		T31.17	T32.5		
CSCvg54850				T32.7	
CSCvf49650		T31.20	T32.6		
CSCvg54853					3.0
CSCvg54856				T32.7	
CSCvf49697		T31.20	T32.6		
CSCvg54861				T32.7	
CSCvf49707		T31.20	T32.7		
CSCvg54867				T32.7	
CSCvf57234		T31.17.2	T32.6		
CSCvg54868					3.0
CSCvg54870				T32.7	

Exploitation and Public Announcements

The Cisco Product Security Incident Response Team (PSIRT) is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

Source

These vulnerabilities were reported to Cisco by Yihan Lian, Fortinet, and Trend Micro as follows:

Cisco Bug IDs	Reporter
CSCve11545, CSCve02843, CSCve11548, CSCve30208, CSCve30214, CSCve30268	Yihan Lian of Qihoo 360 GearTeam
CSCve10584, CSCve10591, CSCve11503, CSCve10658, CSCve11507, CSCve10749, CSCve10744, CSCve11532, CSCve10762, CSCve10764, CSCve11538	Kushal Arvind Shah of Fortinet's Fortiguard Team
CSCvf38077, CSCvg54843, CSCvf38060, CSCvg54836, CSCvf38084, CSCvg54850, CSCvf49650, CSCvg54853, CSCvg54856, CSCvf49697, CSCvg54861, CSCvf49707, CSCvg54867	Steven Seeley of Offensive Security working with Trend Micro's Zero Day Initiative
CSCvf57234, CSCvg54868, CSCvg54870	rgod working with Trend Micro's Zero Day Initiative

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171129-webex-players

---

Revision History

Version	Description	Section	Status	Date
1.3	Provided clarity to first fixed versions.	Fixed Software	Final	2017-November-30
1.2	Updated researcher's information in the Source section.	Source	Final	2017-November-30
1.1	Corrected a bug ID listed in the Details section for CVE-2017-12370.	Details	Final	2017-November-29
1.0	Initial public release.	-	Final	2017-November-29

Legal Disclaimer