



CVE-2019-15285

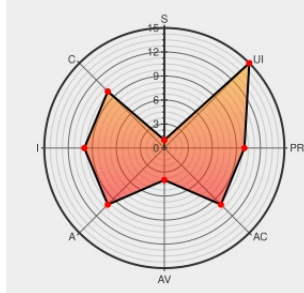
Published on: 09/22/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:45 PM UTC

CVE-2019-15285 - advisory for cisco-sa-20191106-webex-player

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:30/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H



Certain versions of [Webex Meetings](#) from [Cisco](#) contain the following vulnerability:

Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities exist due to insufficient validation of certain elements with a Webex recording stored in either the Advanced

Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit these vulnerabilities by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.

CVE-2019-15285 has been assigned by [Cisco](#) psirt@cisco.com to track the vulnerability - currently rated as **HIGH** severity.

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.

Affected Vendor/Software: [Cisco](#) - **Cisco WebEx WRF Player** version n/a

CVSS3 Score: **7.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **9.3 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE

Confidentiality Impact	Integrity Impact	Availability Impact				
COMPLETE	COMPLETE	COMPLETE				
CVE References						
Description	Tags	Link				
Cisco Webex Network Recording Player and Cisco Webex Player Arbitrary Code Execution Vulnerabilities	Vendor Advisory tools.cisco.com text/html	 CISCO 20191106 Cisco Webex Network Recording Player and Cisco Webex Player Arbitrary Code Execution Vulnerabilities				
By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.						
There are currently no QIDs associated with this CVE						
Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Webex Meetings	All	All	All	All
Application	Cisco	Webex Meetings	All	All	All	All
Application	Cisco	Webex Meetings Online	All	All	All	All
Application	Cisco	Webex Meetings Online	32.11	All	All	All
Application	Cisco	Webex Meetings Online	39.4.0	All	All	All
Application	Cisco	Webex Meetings Online	t32.9	All	All	All
Application	Cisco	Webex Meetings Online	t39.3	All	All	All
Application	Cisco	Webex Meetings Online	t39.6.0	All	All	All
Application	Cisco	Webex Meetings Online	All	All	All	All
Application	Cisco	Webex Meetings Online	32.11	All	All	All
Application	Cisco	Webex Meetings Online	39.4.0	All	All	All
Application	Cisco	Webex Meetings Online	t32.9	All	All	All
Application	Cisco	Webex Meetings Online	t39.3	All	All	All
Application	Cisco	Webex Meetings Online	t39.6.0	All	All	All
Application	Cisco	Webex Meetings Server	3.0	maintenance_release2	All	All
Application	Cisco	Webex Meetings Server	4.0	-	All	All
Application	Cisco	Webex Meetings Server	3.0	maintenance_release2	All	All
Application	Cisco	Webex Meetings Server	4.0	-	All	All
Operating System	Microsoft	Windows	-	All	All	All
Operating	Microsoft	Windows	-	All	All	All

System

cpe:2.3:a:cisco:webex_meetings:~::~::~:

cpe:2.3:a:cisco:webex_meetings:~::~::~:

cpe:2.3:a:cisco:webex_meetings_online:~::~::~:

cpe:2.3:a:cisco:webex_meetings_online:32.11:~::~::~:

cpe:2.3:a:cisco:webex_meetings_online:39.4.0:~::~::~:

cpe:2.3:a:cisco:webex_meetings_online:t32.9:~::~::~:

cpe:2.3:a:cisco:webex_meetings_online:t39.3:~::~::~:

cpe:2.3:a:cisco:webex_meetings_online:t39.6.0:~::~::~:

cpe:2.3:a:cisco:webex_meetings_online:~::~::~:

cpe:2.3:a:cisco:webex_meetings_online:32.11:~::~::~:

cpe:2.3:a:cisco:webex_meetings_online:39.4.0:~::~::~:

cpe:2.3:a:cisco:webex_meetings_online:t32.9:~::~::~:

cpe:2.3:a:cisco:webex_meetings_online:t39.3:~::~::~:

cpe:2.3:a:cisco:webex_meetings_online:t39.6.0:~::~::~:

cpe:2.3:a:cisco:webex_meetings_server:3.0:maintenance_release2:~::~::~:

cpe:2.3:a:cisco:webex_meetings_server:4.0:-:~::~::~:

cpe:2.3:a:cisco:webex_meetings_server:3.0:maintenance_release2:~::~::~:

cpe:2.3:a:cisco:webex_meetings_server:4.0:-:~::~::~:

cpe:2.3:o:microsoft:windows:-:~::~::~:

cpe:2.3:o:microsoft:windows:-:~::~::~:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023  |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

