



CVE-2020-3604

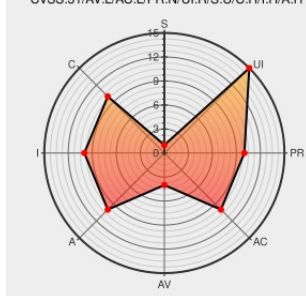
Published on: 11/06/2020 12:00:00 AM UTC

Last Modified on: 11/07/2023 03:23:00 AM UTC

CVE-2020-3604 - advisory for cisco-sa-webex-nbr-NOS6FQ24

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

CVSS:31/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 Windows and Cisco Webex Player for Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities are due to insufficient validation of certain elements of a Webex recording that is stored in the Advanced Recording Format (ARF) or 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-2020-3604 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 vulnerabilities that are described in this advisory.

Affected Vendor/Software: [Cisco](#) **Cisco - Cisco Webex Network Recording 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
ZDI-20-1363 Zero Day Initiative	Third Party Advisory VDB Entry www.zerodayinitiative.com text/html	MISC www.zerodayinitiative.com/advisories/ZDI-20-1363/
Cisco Webex Network Recording Player and Cisco Webex Player Arbitrary Code Execution Vulnerabilities	Vendor Advisory tools.cisco.com text/html	CISCO 20201104 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

cpe:2.3:a:cisco:webex_meetings:*****:

cpe:2.3:a:cisco:webex_meetings:*****:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
--------	-------	--------------

← Previous ID

Next ID →