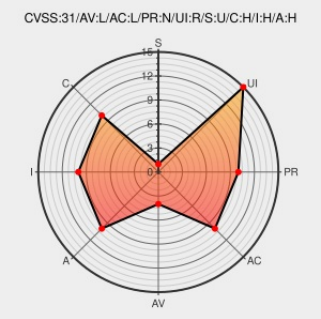
CVE-2020-3573

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

Last Modified on: 10/19/2021 02:48:00 PM UTC

CVE-2020-3573 - advisory for cisco-sa-webex-nbr-NOS6FQ24

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



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-2020-3573 has been assigned by 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 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-20-1362 | Zero Day Initiative	Third Party Advisory VDB Entry www.zerodayinitiative.com text/html	MISC www.zerodayinitiative.com/advisories/ZDI-20-1362/
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

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 Server	3.0	-	All	All
Application	Cisco	Webex Meetings Server	3.0	maintenance_release2	All	All
Application	Cisco	Webex Meetings Server	3.0	maintenance_release3	All	All
Application	Cisco	Webex Meetings Server	3.0	maintenance_release3_service_pack_2	All	All
Application	Cisco	Webex Meetings Server	3.0	maintenance_release3_service_pack_3	All	All
Application	Cisco	Webex Meetings Server	4.0	-	All	All
Application	Cisco	Webex Meetings Server	4.0	maintenance_release1	All	All
Application	Cisco	Webex Meetings Server	4.0	maintenance_release2	All	All
Application	Cisco	Webex Meetings Server	3.0	-	All	All
Application	Cisco	Webex Meetings Server	3.0	maintenance_release2	All	All
Application	Cisco	Webex Meetings Server	3.0	maintenance_release3	All	All
Application	Cisco	Webex Meetings Server	3.0	maintenance_release3_service_pack_2	All	All
Application	Cisco	Webex Meetings Server	3.0	maintenance_release3_service_pack_3	All	All
Application	Cisco	Webex Meetings Server	4.0	-	All	All
Application	Cisco	Webex Meetings Server	4.0	maintenance_release1	All	All
Application	Cisco	Webex Meetings Server	4.0	maintenance_release2	All	All

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

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

cpe:2.3:a:cisco:webex_meetings_server:3.0:-:*:*:*:*:*:*:

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

cpe:2.3:a:cisco:webex_meetings_server:3.0:maintenance_release3:*:*:*:*:*:*:

cpe:2.3:a:cisco:webex_meetings_server:3.0:maintenance_release3_service_pack_2:*:*:*:*:*:*:

cpe:2.3:a:cisco:webex_meetings_server:3.0:maintenance_release3_service_pack_3:*:*:*:*:*:*:

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

cpe:2.3:a:cisco:webex_meetings_server:4.0:maintenance_release1:*:*:*:*:*:*:

cpe:2.3:a:cisco:webex_meetings_server:4.0:maintenance_release2:*:*:*:*:*:*:

cpe:2.3:a:cisco:webex_meetings_server:3.0:-:*:*:*:*:*:*:

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

cpe:2.3:a:cisco:webex_meetings_server:3.0:maintenance_release3:*:*:*:*:*:*:

cpe:2.3:a:cisco:webex_meetings_server:3.0:maintenance_release3_service_pack_2:*:*:*:*:*:*:

cpe:2.3:a:cisco:webex_meetings_server:3.0:maintenance_release3_service_pack_3:*:*:*:*:*:*:

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

cpe:2.3:a:cisco:webex_meetings_server:4.0:maintenance_release1:*:*:*:*:*:*:

cpe:2.3:a:cisco:webex_meetings_server:4.0:maintenance_release2:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@RexorVc0	#APT #APT28 #FancyBear #Sofacy #Campaign #threat ??? ????? #Phishing (News Of Ukraine Subject) > CVE-2020-3573… twitter.com/i/web/status/1…	2023-06-22 06:12:11

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report