



CVE-2018-15430

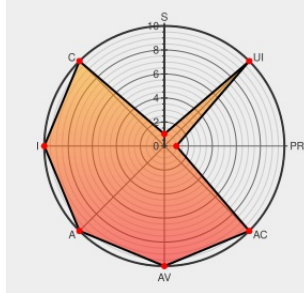
Published on: 10/05/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:27 PM UTC

CVE-2018-15430 - advisory for cisco-sa-20181003-express-vcs-rce

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

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



Certain versions of [Telepresence Video Communication Server](#) from [Cisco](#) contain the following vulnerability:

A vulnerability in the administrative web interface of Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) could allow an authenticated, remote attacker to execute code with user-level privileges on the underlying operating system. The vulnerability is due to insufficient validation of the content of upgrade

packages. An attacker could exploit this vulnerability by uploading a malicious archive to the Upgrade page of the administrative web interface. A successful exploit could allow the attacker to execute code with user-level privileges on the underlying operating system.

CVE-2018-15430 has been assigned by [cisco](#) psirt@cisco.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [cisco](#) **Cisco - Cisco TelePresence Video Communication Server (VCS)** version n/a

CVSS3 Score: **7.2 - HIGH**

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

CVSS2 Score: **6.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Cisco Expressway Series and Cisco TelePresence Video Communication Server Remote Code Execution Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20181003 Cisco Expressway Series and Cisco TelePresence Video Communication Server Remote Code Execution Vulnerability
Cisco TelePresence Video Communication Server Upgrade Package Validation Flaw Lets Remote Authenticated Users Execute Arbitrary Code on the Target System - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTrack 1041784

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	Telepresence Video Communication Server	x7.2.4	All	All	All
Application	Cisco	Telepresence Video Communication Server	x8.10.4	All	All	All
Application	Cisco	Telepresence Video Communication Server	x8.9.2	All	All	All
Application	Cisco	Telepresence Video Communication Server	x7.2.4	All	All	All
Application	Cisco	Telepresence Video Communication Server	x8.10.4	All	All	All
Application	Cisco	Telepresence Video Communication Server	x8.9.2	All	All	All

cpe:2.3:a:cisco:telepresence_video_communication_server:x7.2.4:*****:

cpe:2.3:a:cisco:telepresence_video_communication_server:x8.10.4:*****:

cpe:2.3:a:cisco:telepresence_video_communication_server:x8.9.2:*****:

cpe:2.3:a:cisco:telepresence_video_communication_server:x7.2.4:*****:

cpe:2.3:a:cisco:telepresence_video_communication_server:x8.10.4:*****:

cpe:2.3:a:cisco:telepresence_video_communication_server:x8.9.2:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)