



CVE-2017-6681

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2017-6681
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-06-13 06:29:00 UTC
Updated	2017-06-21 15:34:00 UTC
Description	A vulnerability in the AutoVNF VNFStagingView class of Cisco Ultra Services Framework could allow an unauthenticated, remote attacker to execute arbitrary code on the target device. The vulnerability is due to a buffer overflow in the VNFStagingView class. An attacker could exploit this vulnerability to execute arbitrary code on the target device. The vulnerability is present in Cisco Ultra Services Framework versions 21.0.0 through 21.0.0. Cisco is currently investigating this vulnerability and has released a patch to address the issue. Cisco recommends that users of Cisco Ultra Services Framework upgrade to the latest version of the software as soon as possible.

Risk And Classification

Problem Types: CWE-22 | CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Ultra Services Framework	21.0.0	All	All	All
Application	Cisco	Ultra Services Framework	21.0.0	All	All	All

References

Reference	Source	Link	Tag
Cisco Ultra Services Framework CVE-2017-6681 Information Disclosure Vulnerability	BID	www.securityfocus.com	Third Party
Cisco Ultra Services Framework AutoVNF VNFStagingView Information Disclosure Vulnerability	CONFIRM	tools.cisco.com	Vendor
CVE Program record	CVE.ORG	www.cve.org	Canonical
NVD vulnerability detail	NVD	nvd.nist.gov	Canonical

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#).

Free CVE JSON API cve.report/api

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