



CVE-2017-6680

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

Summary

CVE	CVE-2017-6680
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 16:29:00 UTC
Description	A vulnerability in the AutoVNF logging function of Cisco Ultra Services Framework could allow an unauthenticated, remote attacker to execute arbitrary code with root privileges on the affected device.

Risk And Classification

Problem Types: CWE-20

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	Tags
Cisco Ultra Services Framework AutoVNF Arbitrary Direction Creation Vulnerability	CONFIRM	tools.cisco.com	Vendor Advisory
Cisco Ultra Services Framework CVE-2017-6680 Remote Security Bypass Vulnerability	BID	www.securityfocus.com	Third Party
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, authoritative

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