



CVE-2017-6704

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

Summary

CVE	CVE-2017-6704
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-07-04 00:29:00 UTC
Updated	2017-07-07 17:29:00 UTC
Description	A vulnerability in the web application in the Cisco Prime Collaboration Provisioning tool could allow an authenticated, remot

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Prime Collaboration Provisioning	12.1	All	All	All
Application	Cisco	Prime Collaboration Provisioning	12.1	All	All	All

References

Reference
Cisco Prime Collaboration Provisioning Tool Bugs Let Remote Users Hijack Sessions, Remote Authenticated Users Download Files, and Local
Cisco Prime Collaboration Provisioning Tool Arbitrary File Download Vulnerability
Cisco Prime Collaboration Provisioning CVE-2017-6704 Arbitrary File Download Vulnerability
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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](#).

Free CVE JSON API cve.report/api

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