



CVE-2018-0321

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

Summary

CVE	CVE-2018-0321
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-06-07 12:29:00 UTC
Updated	2019-10-09 23:31:00 UTC
Description	A vulnerability in Cisco Prime Collaboration Provisioning (PCP) could allow an unauthenticated, remote attacker to access t

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Lin
Cisco Prime Collaboration Provisioning Open NICE Port Lets Remote Users Access the Target System - SecurityTracker	SECTRACK	ww
Malformed Request	BID	ww
Cisco Prime Collaboration Provisioning Unauthenticated Remote Method Invocation Vulnerability	CONFIRM	too
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvc

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#).

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