



# CVE-2018-0336

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2018-0336
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@cisco.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-06-07 21:29:00 UTC
<b>Updated</b>	2019-10-09 23:31:00 UTC
<b>Description</b>	A vulnerability in the batch provisioning feature of Cisco Prime Collaboration Provisioning could allow an authenticated, remote user to escalate their privileges to administrative level. This vulnerability is present in Cisco Prime Collaboration Provisioning versions 12.1(1) through 12.1(100). Cisco has released a software update to address this vulnerability. Cisco Prime Collaboration Provisioning versions 12.1(101) through 12.1(1000) are not affected by this vulnerability.

## Risk And Classification

**Problem Types:** CWE-862

## NVD Known Affected Configurations (CPE 2.3)

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

## References

### Reference

- Cisco Prime Collaboration Provisioning Access Control Deficiency in Batch Function Privilege Escalation Vulnerability
- Cisco Prime Collaboration Provisioning CVE-2018-0336 Remote Privilege Escalation Vulnerability
- Cisco Prime Collaboration Provisioning Batch Provisioning Bug Lets Remote Authenticated Users Gain Elevated Privileges - SecurityTracker
- 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](#).

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