



CVE-2018-0124

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2018-0124
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-02-22 00:29:00 UTC
Updated	2019-10-09 23:31:00 UTC
Description	A vulnerability in Cisco Unified Communications Domain Manager could allow an unauthenticated, remote attacker to bypass

Risk And Classification

Problem Types: CWE-320

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Unified Communications Domain Manager	All	All	All	All
Application	Cisco	Unified Communications Domain Manager	All	All	All	All

References

Reference

- Cisco Unified Communications Domain Manager CVE-2018-0124 Remote Code Execution Vulnerability
- Cisco Unified Communications Domain Manager Remote Code Execution Vulnerability
- Cisco Unified Communications Domain Manager Insecure Key Generation Lets Remote Users Execute Arbitrary Code on the Target System
- 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](#)