



CVE-2018-0266

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2018-0266
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-04-19 20:29:00 UTC
Updated	2020-09-04 18:28:00 UTC
Description	A vulnerability in the web framework of Cisco Unified Communications Manager could allow an authenticated, remote attack

Risk And Classification

Problem Types: CWE-425

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Unified Communications Manager	10.5(2.10000.5)	All	All	All
Application	Cisco	Unified Communications Manager	10.5(2.10000.5\)	All	All	All
Application	Cisco	Unified Communications Manager	11.0(1.10000.10)	All	All	All
Application	Cisco	Unified Communications Manager	11.0(1.10000.10\)	All	All	All
Application	Cisco	Unified Communications Manager	11.5(1.10000.6)	All	All	All
Application	Cisco	Unified Communications Manager	11.5(1.10000.6\)	All	All	All
Application	Cisco	Unified Communications Manager	12.0(1.10000.10)	All	All	All
Application	Cisco	Unified Communications Manager	12.0(1.10000.10\)	All	All	All
Application	Cisco	Unified Communications Manager	10.5(2.10000.5\)	All	All	All
Application	Cisco	Unified Communications Manager	11.0(1.10000.10\)	All	All	All
Application	Cisco	Unified Communications Manager	11.5(1.10000.6\)	All	All	All
Application	Cisco	Unified Communications Manager	12.0(1.10000.10\)	All	All	All

References

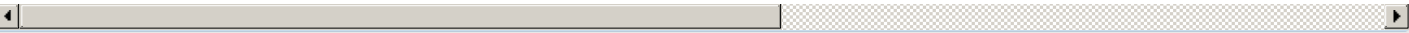
Reference

Cisco Unified Communications Manager HTTP Interface Information Disclosure Vulnerability

Cisco Unified Communications Manager HTTP Access Control Flaw Lets Remote Authenticated Users Obtain Potentially Sensitive Information

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.

© [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](#).

Free CVE JSON API [cve.report/api](#)

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