



CVE-2015-4206

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary

CVE	CVE-2015-4206
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-12-15 05:59:00 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Cisco Unified Communications Manager (UCM) 8.0 through 8.6 allows remote attackers to bypass an XSS protection mechanism.

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

AV:N/AC:M/Au:N/C:N/I:P/A:N

Problem Types: CWE-79 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:M/Au:N/C:N/I:P/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Unified Communications Manager	8.0(2c\)	All	All	All

Application	Cisco	Unified Communications Manager	8.0\3\	All	All	All
Application	Cisco	Unified Communications Manager	8.0_base	All	All	All
Application	Cisco	Unified Communications Manager	8.5.1	All	All	All
Application	Cisco	Unified Communications Manager	8.5_base	All	All	All
Application	Cisco	Unified Communications Manager	8.6.1	All	All	All
Application	Cisco	Unified Communications Manager	8.6.2	All	All	All
Application	Cisco	Unified Communications Manager	8.6_base	All	All	All

Vendor Declared Affected Products					
Source	Vendor	Product	Version	Platforms	
CNA	Na	N/a	affected n/a	Not specified	

References
Reference
Cisco Unified Communications Manager Input Validation Flaw in Web Management Interface Lets Remote Conduct Cross-Site Scripting Attac
Cisco Unified Communications Manager Cross-Site Scripting Filter Security Bypass Vulnerability
Cisco Unified Communications Manager Web Management Interface Cross-Site Scripting Filter Bypass 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.