CVE-2009-0057

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

Summary

CVE	CVE-2009-0057
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-01-22 18:30:03 UTC
Updated	2026-04-23 00:35:47 UTC
Description	The Certificate Authority Proxy Function (CAPF) service in Cisco Unified Communications Manager 5.x before 5.1(3e) and

Risk And Classification

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

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

Problem Types: CWE-20 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Unified Communications Manager	5.0	All	All	All

Application	Cisco	Unified Communications Manager	5.0_1	All	All	All
Application	Cisco	Unified Communications Manager	5.0_2	All	All	All
Application	Cisco	Unified Communications Manager	5.0_3	All	All	All
Application	Cisco	Unified Communications Manager	5.0_3a	All	All	All
Application	Cisco	Unified Communications Manager	5.0_4	All	All	All
Application	Cisco	Unified Communications Manager	5.0_4a	All	All	All
Application	Cisco	Unified Communications Manager	5.0_4a_su1	All	All	All
Application	Cisco	Unified Communications Manager	5.1	All	All	All
Application	Cisco	Unified Communications Manager	5.1	5.1\(1\)	All	All
Application	Cisco	Unified Communications Manager	5.1	5.1_\(2a\)	All	All
Application	Cisco	Unified Communications Manager	5.1	\(1\)	All	All
Application	Cisco	Unified Communications Manager	5.1	\(2a\)	All	All
Application	Cisco	Unified Communications Manager	5.1	\(2b\)	All	All
Application	Cisco	Unified Communications Manager	5.1	\(2\)	All	All
Application	Cisco	Unified Communications Manager	5.1	\(3a\)	All	All
Application	Cisco	Unified Communications Manager	5.1.2	All	All	All
Application	Cisco	Unified Communications Manager	5.1\(1\)	All	All	All
Application	Cisco	Unified Communications Manager	5.1\(2\)	All	All	All
Application	Cisco	Unified Communications Manager	5.1\(3c\)	All	All	All
Application	Cisco	Unified Communications Manager	5.1_1	All	All	All
Application	Cisco	Unified Communications Manager	5.1_2	All	All	All
Application	Cisco	Unified Communications Manager	5.1_2a	All	All	All
Application	Cisco	Unified Communications Manager	5.1_2b	All	All	All
Application	Cisco	Unified Communications Manager	5.1_3a	All	All	All
Application	Cisco	Unified Communications Manager	5.1_\(2a\)	All	All	All
Application	Cisco	Unified Communications Manager	6.0	All	All	All
Application	Cisco	Unified Communications Manager	6.0	\(1a\)	All	All
Application	Cisco	Unified Communications Manager	6.0	\(1\)	All	All
Application	Cisco	Unified Communications Manager	6.0_1	All	All	All
Application	Cisco	Unified Communications Manager	6.0_1a	All	All	All
Application	Cisco	Unified Communications Manager	6.1	All	All	All
Application	Cisco	Unified Communications Manager	6.1	\(1a\)	All	All
Application	Cisco	Unified Communications Manager	6.1.0	All	All	All
Application	Cisco	Unified Communications Manager	6.1\(2\)	All	All	All
Application	Cisco	Unified Communications Manager	6.1_1a	All	All	All

Vendor Declared Affected Products

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

References

Reference
IBM X-Force Exchange
Cisco Security Advisory: Cisco Unified Communications Manager CAPF Denial of Service Vulnerability [Products & Services] - Cisco Systems
Cisco Unified Communications Manager CAPF Denial of Service - Secunia Advisories - Vulnerability Information - Secunia.com
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Cisco Unified Communications Manager CAPF Service Denial of Service Vulnerability
Cisco Unified Communications Manager Input Validation Flaw in Certificate Authority Proxy Function Lets Remote Users Deny Service - Secu
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.