Cisco Integrated Management Controller Cross-Site Scripting Vulnerability

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-20085
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-01 17:28:26 UTC
Updated	2026-04-03 16:11:11 UTC
Description	A vulnerability in the web-based management interface of Cisco IMC could allow an unauthenticated, remote attacker to co

Risk And Classification

Primary CVSS: v3.1 6.1 MEDIUM from psirt@cisco.com

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

EPSS: 0.000200000 probability, percentile 0.054500000 (date 2026-04-02)

Problem Types: CWE-79 | CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
3.1	psirt@cisco.com	Primary	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
3.1	CNA	CVSSV3_1	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

Low

ntegrity

Low

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.1.1	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 3.9.1	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 3.5.2	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 3.12.2	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 3.6.2	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 3.9.2	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 3.11.3	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 3.11.1	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 3.5.1	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 3.3.1	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 3.10.2	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 3.12.1b	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 3.4.1	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 3.12.1a	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 3.6.3	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 3.8.1	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 3.11.2	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 3.12.1	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 3.12.3	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 3.10.1	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 3.6.1	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 3.10.3	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 3.7.1	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.1.2	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.2.1	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.2.2	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.4.1	Not specified

CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.4.2	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.5.1	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.4.3	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.6.1	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.7.1	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.6.2-FC2	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.6.2-FC3	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.6.2	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.8.1	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.8.2	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.9.1	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.6.3	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.9.2-FC5	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.9.2	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.10.1	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.9.3	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.11.1	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.9.4	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.12.1	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.6.4	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.12.2	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.13.1	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.9.4-ES8	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.9.5	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.12.3	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.6.5-ES1	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.9.4-ES9	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.14.1	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.6.3-FC4	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.9.4-FC3	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.12.4	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.15.1	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.9.6	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.16.1	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.15.2	Not specified

CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.12.5	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.15.3	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.15.4	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.18.1	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.12.6	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.18.2	Not specified
CNA	Cisco	Cisco Enterprise NFV Infrastructure Software	affected 4.18.2a	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.0(2g)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 3.1(2i)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 3.1(1d)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.0(4i)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.1(1c)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.0(2c)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.0(1e)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.0(2h)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.0(4h)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.0(1h)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.0(2l)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 3.1(3g)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.0(1.240)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.0(2f)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.0(1g)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.0(2i)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 3.1(3i)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.0(4d)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.1(1d)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 3.1(3c)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.0(4k)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 3.1(2d)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 3.1(3a)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 3.1(3j)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.0(2d)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.1(1f)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.0(1c)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.0(4f)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.0(4c)	Not specified

CNA	Cisco	Cisco Unified Computing System Standalone	affected 3.1(3d)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 3.1(2g)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 3.1(2c)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.0(1d)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 3.1(2e)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.0(1a)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.0(1b)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 3.1(3b)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.0(4b)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 3.1(2b)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.0(4e)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 3.1(3h)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.0(4l)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.1(1g)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.1(2a)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.0(2n)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.1(1h)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 3.1(3k)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.1(2b)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.0(2o)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.0(4m)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.1(2d)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.1(3b)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.0(2p)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.1(2e)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.1(2f)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.0(4n)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.0(2q)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.1(3c)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.0(2r)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.1(3d)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.1(2g)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.1(2h)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.1(3f)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.1(2j)	Not specified

CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.1(2k)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.1(3h)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.2(2a)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.1(3i)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.2(2f)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.2(2g)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.2(3b)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.1(3l)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.2(3d)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.3(1.230097)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.2(1e)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.2(1b)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.2(1j)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.2(1i)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.2(1f)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.2(1a)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.2(1c)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.2(1g)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.3(1.230124)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.1(2l)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.2(3e)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.3(1.230138)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.2(3g)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.3(2.230207)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.2(3h)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.2(3i)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.3(2.230270)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.1(3m)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.1(2m)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.3(2.240002)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.3(3.240022)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.2(3j)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.1(3n)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.3(2.240009)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.3(3.240043)	Not specified

CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.3(4.240142)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.3(2.240037)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.3(2.240053)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.3(4.240152)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.2(3l)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.3(2.240077)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.3(4.242028)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.3(4.241063)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.3(4.242038)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.2(3m)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.3(2.240090)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.3(5.240021)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.3(2.240107)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.3(4.242066)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.2(3n)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.3(5.250001)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.2(3o)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.3(2.250016)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.3(2.250021)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.3(5.250030)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.3(2.250022)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.3(6.250040)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.3(5.250033)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.3(6.250044)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.3(6.250053)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.3(2.250037)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.3(2.250045)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.3(4.252001)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.3(4.252002)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 6.0(1.250127)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.2(3p)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 6.0(1.250131)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.3(6.250101)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 6.0(1.250174)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.3(6.250117)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.3(5.250043)	Not specified

CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.3(6.250039)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.3(5.250045)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.3(6.250060)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 6.0(1.250130)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.3(4.241014)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.3(2.250063)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 6.0(1.250192)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 4.3(6.260003)	Not specified
CNA	Cisco	Cisco Unified Computing System Standalone	affected 6.0(1.250194)	Not specified
CNA	Cisco	Cisco Unified Computing System E-Series Software UCSE	affected 3.2.7	Not specified
CNA	Cisco	Cisco Unified Computing System E-Series Software UCSE	affected 3.2.6	Not specified
CNA	Cisco	Cisco Unified Computing System E-Series Software UCSE	affected 3.2.4	Not specified
CNA	Cisco	Cisco Unified Computing System E-Series Software UCSE	affected 3.2.10	Not specified
CNA	Cisco	Cisco Unified Computing System E-Series Software UCSE	affected 3.2.2	Not specified
CNA	Cisco	Cisco Unified Computing System E-Series Software UCSE	affected 3.2.3	Not specified
CNA	Cisco	Cisco Unified Computing System E-Series Software UCSE	affected 2.4.0	Not specified
CNA	Cisco	Cisco Unified Computing System E-Series Software UCSE	affected 3.2.1	Not specified
CNA	Cisco	Cisco Unified Computing System E-Series Software UCSE	affected 3.2.11.1	Not specified
CNA	Cisco	Cisco Unified Computing System E-Series Software UCSE	affected 3.2.8	Not specified
CNA	Cisco	Cisco Unified Computing System E-Series Software UCSE	affected 3.1.1	Not specified
CNA	Cisco	Cisco Unified Computing System E-Series Software UCSE	affected 3.0.2	Not specified
CNA	Cisco	Cisco Unified Computing System E-Series Software UCSE	affected 2.1.0	Not specified
CNA	Cisco	Cisco Unified Computing System E-Series Software UCSE	affected 2.2.2	Not specified
CNA	Cisco	Cisco Unified Computing System E-Series Software UCSE	affected 3.1.2	Not specified
CNA	Cisco	Cisco Unified Computing System E-Series Software UCSE	affected 3.0.1	Not specified
CNA	Cisco	Cisco Unified Computing System E-Series Software UCSE	affected 2.3.2	Not specified
CNA	Cisco	Cisco Unified Computing System E-Series Software UCSE	affected 2.3.5	Not specified
CNA	Cisco	Cisco Unified Computing System E-Series Software UCSE	affected 2.2.1	Not specified
CNA	Cisco	Cisco Unified Computing System E-Series Software UCSE	affected 3.1.4	Not specified
CNA	Cisco	Cisco Unified Computing System E-Series Software UCSE	affected 2.4.1	Not specified
CNA	Cisco	Cisco Unified Computing System E-Series Software UCSE	affected 2.3.1	Not specified
CNA	Cisco	Cisco Unified Computing System E-Series Software UCSE	affected 3.1.3	Not specified
CNA	Cisco	Cisco Unified Computing System E-Series Software UCSE	affected 2.3.3	Not specified
CNA	Cisco	Cisco Unified Computing System E-Series Software UCSE	affected 2.4.2	Not specified
CNA	Cisco	Cisco Unified Computing System E-Series Software UCSE	affected 3.1.5	Not specified

CNA	Cisco	Cisco Unified Computing System E-Series Software UCSE	affected 3.1.0	Not specified
CNA	Cisco	Cisco Unified Computing System E-Series Software UCSE	affected 2.0.0	Not specified
CNA	Cisco	Cisco Unified Computing System E-Series Software UCSE	affected 3.2.11.3	Not specified
CNA	Cisco	Cisco Unified Computing System E-Series Software UCSE	affected 3.2.11.5	Not specified
CNA	Cisco	Cisco Unified Computing System E-Series Software UCSE	affected 3.2.12.2	Not specified
CNA	Cisco	Cisco Unified Computing System E-Series Software UCSE	affected 3.2.13.6	Not specified
CNA	Cisco	Cisco Unified Computing System E-Series Software UCSE	affected 3.2.14	Not specified
CNA	Cisco	Cisco Unified Computing System E-Series Software UCSE	affected 4.11.1	Not specified
CNA	Cisco	Cisco Unified Computing System E-Series Software UCSE	affected 3.2.15	Not specified
CNA	Cisco	Cisco Unified Computing System E-Series Software UCSE	affected 4.12.1	Not specified
CNA	Cisco	Cisco Unified Computing System E-Series Software UCSE	affected 3.2.15.3	Not specified
CNA	Cisco	Cisco Unified Computing System E-Series Software UCSE	affected 4.12.2	Not specified
CNA	Cisco	Cisco Unified Computing System E-Series Software UCSE	affected 3.2.16.1	Not specified
CNA	Cisco	Cisco Unified Computing System E-Series Software UCSE	affected 4.00	Not specified
CNA	Cisco	Cisco Unified Computing System E-Series Software UCSE	affected 4.15.2	Not specified
CNA	Cisco	Cisco Unified Computing System E-Series Software UCSE	affected 4.02	Not specified

References

Reference	Source	Link	Ta
sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-x...	psirt@cisco.com	sec.cloudapps.cisco.com	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Exploits

CNA: The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerabilities that are described in this advisory.

There are currently no legacy QID mappings associated with this CVE.

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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