CVE-2014-7996

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

Summary

CVE	CVE-2014-7996
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-11-18 23:59:04 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Cross-site request forgery (CSRF) vulnerability in the web framework in Cisco Integrated Management Controller in Cisco U

Risk And Classification

Primary CVSS: v2.0 6.8 from nvd@nist.gov

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

Problem Types: CWE-352 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Unified Computing System	-	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
Security Advisory SA62565 - Cisco Unified Computing System (UCS) Cross-Site Request Forgery Vulnerability - Secunia	af854a3a-2127-4
tools.cisco.com/security/center/viewAlert.x	af854a3a-2127-4
tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-7996	af854a3a-2127-4
IBM X-Force Exchange	af854a3a-2127-4
Cisco Unified Computing System CVE-2014-7996 Cross Site Request Forgery Vulnerability	af854a3a-2127-4
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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