



CVE-2014-0725

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2014-0725
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-02-13 05:24:51 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Cisco Unified Communications Manager (UCM) does not require authentication for reading WAR files, which allows remote

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

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

EPSS: 0.002750000 probability, percentile 0.508700000 (date 2026-05-05)

Problem Types: CWE-287 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
------	--------	---------	---------	--------	---------	----------

Application	Cisco	Unified Communications Manager	All	All	All	All
Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		
References						
Reference	Source		Link			
tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-0725	af854a3a-2127-422b-91ae-364da2661108		tools.cisco.com			
CVE Program record	CVE.ORG		www.cve.org			
NVD vulnerability detail	NVD		nvd.nist.gov			
No vendor comments have been submitted for this CVE.						
There are currently no legacy QID mappings associated with this CVE.						