CVE-2014-3305

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

Summary

CVE	CVE-2014-3305
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-07-26 11:11:57 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Cross-site request forgery (CSRF) vulnerability in the web framework in Cisco WebEx Meetings Server 1.5(.1.131) and earl

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
Application	Cisco	Webex Meetings Server	1.5	All	All	All

Application	Cisco	Webex Meetings Server	1.5\(.1.6\)	All	All	All
Application	Cisco	Webex Meetings Server	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
Alert Details - Security Center - Cisco Systems	af854a3a-2127-422b-91
IBM X-Force Exchange	af854a3a-2127-422b-91
Cisco WebEx Meetings Server Input Validation Flaw Permits Cross-Site Request Forgery Attacks - SecurityTracker	af854a3a-2127-422b-91
Cisco WebEx Meetings Server CVE-2014-3305 Cross Site Request Forgery Vulnerability	af854a3a-2127-422b-91
Alert Details - Security Center - Cisco Systems	af854a3a-2127-422b-91
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.