CVE-2015-0747

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

Summary

CVE	CVE-2015-0747
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-05-30 14:59:04 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Cisco Conductor for Videoscape 3.0 and Cisco Headend System Release allow remote attackers to inject arbitrary cookies

Risk And Classification

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

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

Problem Types: CWE-20 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Headend Digital Broadband Delivery System	-	All	All	All

Operating System	Cisco	Headend System Release	2.5	All	All	All
Operating System	Cisco	Headend System Release	2.7	All	All	All
Operating System	Cisco	Headend System Release	3.2	All	All	All
Operating System	Cisco	Headend System Release	3.5	All	All	All
Operating System	Cisco	Headend System Release	3.7	All	All	All
Operating System	Cisco	Headend System Release	i4.3	All	All	All
Application	Cisco	Videoscape Conductor	3.0	All	All	All

Vendor Declared Affected Products

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

References

Reference	Sou
Cisco Headend Digital Broadband Delivery System Bug Lets Remote Users Conduct HTTP Header Injection Attacks - SecurityTracker	af85
Cisco Conductor for Videoscape and Cisco Headend System Release HTTP Injection Vulnerability	af85
CVE Program record	CVE
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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