



CVE-2015-0759

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

Summary

CVE	CVE-2015-0759
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-06-02 14:59:02 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Cross-site request forgery (CSRF) vulnerability in Cisco Headend Digital Broadband Delivery System allows remote attacker

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-20 | 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
Operating System	Cisco	Headend Digital Broadband Delivery System	-	All	All	All

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified
References				
Reference				
Cisco Headend Digital Broadband Delivery System Input Validation Flaw Lets Remote Users Conduct Cross-Site Request Forgery Attacks - S				
Cisco Headend Digital Broadband Delivery System Cross-Site Request Forgery Vulnerability				
CVE Program record				
NVD vulnerability detail				
No vendor comments have been submitted for this CVE.				
There are currently no legacy QID mappings associated with this CVE.				