CVE-2015-0744

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

Summary

CVE	CVE-2015-0744
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-05-30 14:59:02 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Cisco DTA Control System (DTACS) 4.0.0.9 and Cisco Headend System Release allow remote attackers to cause a denial

Risk And Classification

Primary CVSS: v2.0 7.8 from nvd@nist.gov

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

Problem Types: CWE-399 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Dta Control System	4.0.0.9	All	All	All

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

Vendor Declared Affected Products

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

References

Reference	Source
Multiple Cisco Products CVE-2015-0744 Denial of Service Vulnerability	af854a
Multiple Cisco Products TCP Flood Denial of Service Vulnerability	af854a
Cisco Headend System Bugs Let Remote Users Conduct HTTP Response Splitting and Denial of Service Attacks - SecurityTracker	af854a
CVE Program record	CVE.O
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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