CVE-2015-0754

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

Summary

CVE	CVE-2015-0754
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-05-29 15:59:08 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Cisco Finesse 10.5(1) allows remote authenticated users to obtain sensitive information or cause a denial of service (CPU a

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

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

Problem Types: CWE-20 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

Single

Confidentiality

Partial

Integrity

None

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Finesse	10.5\(1\)_base	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
Cisco Finesse XML Processing Denial of Service Vulnerability	af854a3a-2127-422b-91ae-364da2
Cisco Finesse XML Processing Flaw Lets Remote Authenticated Users Deny Service - SecurityTracker	af854a3a-2127-422b-91ae-364da2
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.