CVE-2013-3455

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

Summary

CVE	CVE-2013-3455
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-08-12 10:58:49 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Cisco Finesse allows remote attackers to obtain sensitive information by sniffing the network for HTTP query data, aka Bug

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

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

Problem Types: CWE-255 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Finesse	-	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 Discloses Potentially Sensitive Information in Query Parameters - SecurityTracker	af854a3a-2127-422b-91ae-364da266110
tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2013-3455	af854a3a-2127-422b-91ae-364da266110
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da266110
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.