CVE-2016-1373

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

Summary

CVE	CVE-2016-1373
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-05-05 21:59:03 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The gadgets-integration API in Cisco Finesse 8.5(1) through 8.5(5), 8.6(1), 9.0(1), 9.0(2), 9.1(1), 9.1(1)SU1, 9.1(1)SU1.1, 9

Risk And Classification

Primary CVSS: v3.0 8.6 HIGH from nvd@nist.gov

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:H/A:N

Problem Types: NVD-CWE-Other | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	8.6	HIGH	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:H/A:N
2.0	nvd@nist.gov	Primary	5		AV:N/AC:L/Au:N/C:N/I:P/A:N

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

None

Integrity

High

Availability

None

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:H/A:N

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Finesse	10.0\(1\)_base	All	All	All
Application	Cisco	Finesse	10.0\(1\)_su1	All	All	All
Application	Cisco	Finesse	10.0\(1\)_su1.1	All	All	All
Application	Cisco	Finesse	10.5\(1\)_base	All	All	All
Application	Cisco	Finesse	10.5\(1\)_es1	All	All	All
Application	Cisco	Finesse	10.5\(1\)_es2	All	All	All
Application	Cisco	Finesse	10.5\(1\)_es3	All	All	All
Application	Cisco	Finesse	10.5\(1\)_es4	All	All	All
Application	Cisco	Finesse	10.5\(1\)_su1	All	All	All
Application	Cisco	Finesse	10.5\(1\)_su1.1	All	All	All
Application	Cisco	Finesse	10.5\(1\)_su1.7	All	All	All
Application	Cisco	Finesse	10.6\(1\)_base	All	All	All
Application	Cisco	Finesse	10.6\(1\)_su1	All	All	All
Application	Cisco	Finesse	10.6\(1\)_su2	All	All	All
Application	Cisco	Finesse	11.0\(1\)_base	All	All	All
Application	Cisco	Finesse	8.5\(1\)_base	All	All	All
Application	Cisco	Finesse	8.5\(2\)_base	All	All	All

Application	Cisco	Finesse	8.5\(3\)_base	All	All	All
Application	Cisco	Finesse	8.5\(4\)_base	All	All	All
Application	Cisco	Finesse	8.5\(5\)_base	All	All	All
Application	Cisco	Finesse	8.6\(1\)_base	All	All	All
Application	Cisco	Finesse	9.0\(1\)_base	All	All	All
Application	Cisco	Finesse	9.0\(2\)_base	All	All	All
Application	Cisco	Finesse	9.1\(1\)_base	All	All	All
Application	Cisco	Finesse	9.1\(1\)_es1	All	All	All
Application	Cisco	Finesse	9.1\(1\)_es2	All	All	All
Application	Cisco	Finesse	9.1\(1\)_es3	All	All	All
Application	Cisco	Finesse	9.1\(1\)_es4	All	All	All
Application	Cisco	Finesse	9.1\(1\)_es5	All	All	All
Application	Cisco	Finesse	9.1\(1\)_su1	All	All	All
Application	Cisco	Finesse	9.1\(1\)_su1.1	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 HTTP Request Processing Server-Side Request Forgery Vulnerability	af854a3a-212
Cisco Finesse API Access Control Flaw Lets Remote Users Conduct Server-Side Request Forgery Attacks - SecurityTracker	af854a3a-212
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.

CVE.report and Source URL Uptime Status status.cve.report