CVE-2016-6439

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

Summary

CVE	CVE-2016-6439
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-10-27 21:59:11 UTC
Updated	2026-05-06 22:30:45 UTC
Description	A vulnerability in the detection engine reassembly of HTTP packets for Cisco Firepower System Software before 6.0.1 coul

Risk And Classification

Primary CVSS: v3.0 7.5 HIGH from nvd@nist.gov

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

EPSS: 0.001450000 probability, percentile 0.344730000 (date 2026-05-09)

Problem Types: CWE-399 | unspecified

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
2.0	nvd@nist.gov	Primary	4.3		AV:N/AC:M/Au:N/C:N/I:N/A:P

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

None

Availability

High

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Secure Firewall Management Center	5.3.0	All	All	All
Application	Cisco	Secure Firewall Management Center	5.3.0.2	All	All	All
Application	Cisco	Secure Firewall Management Center	5.3.0.3	All	All	All
Application	Cisco	Secure Firewall Management Center	5.3.0.4	All	All	All
Application	Cisco	Secure Firewall Management Center	5.3.1	All	All	All
Application	Cisco	Secure Firewall Management Center	5.3.1.3	All	All	All
Application	Cisco	Secure Firewall Management Center	5.3.1.4	All	All	All
Application	Cisco	Secure Firewall Management Center	5.3.1.5	All	All	All
Application	Cisco	Secure Firewall Management Center	5.3.1.6	All	All	All
Application	Cisco	Secure Firewall Management Center	5.4.0	All	All	All
Application	Cisco	Secure Firewall Management Center	5.4.0.2	All	All	All
Application	Cisco	Secure Firewall Management Center	5.4.1	All	All	All
Application	Cisco	Secure Firewall Management Center	5.4.1.1	All	All	All
Application	Cisco	Secure Firewall Management Center	5.4.1.2	All	All	All
Application	Cisco	Secure Firewall Management Center	5.4.1.3	All	All	All
Application	Cisco	Secure Firewall Management Center	5.4.1.4	All	All	All

Application	Cisco	Secure Firewall Management Center	5.4.1.5	All	All	All
Application	Cisco	Secure Firewall Management Center	5.4.1.6	All	All	All
Application	Cisco	Secure Firewall Management Center	5.4_base	All	All	All
Application	Cisco	Secure Firewall Management Center	6.0.0	All	All	All
Application	Cisco	Secure Firewall Management Center	6.0.0.0	All	All	All
Application	Cisco	Secure Firewall Management Center	6.0.0.1	All	All	All
Application	Cisco	Secure Firewall Management Center	6.0.1	All	All	All
Application	Cisco	Secure Firewall Management Center	6.0_base	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	Cisco Firepower System Software Before 6.0.1	affected Cisco Firepower System Software before 6.0.1	Not specified

References

Reference	Sour
Cisco Firepower Detection Engine HTTP Denial of Service Vulnerability	af854
Multiple Cisco Products CVE-2016-6439 Denial of Service Vulnerability	af854
Cisco ASA 5500-X Series with FirePOWER Services Lets Remote Users Cause the Target Snort Service to Restart - SecurityTracker	af854
CVE Program record	CVE.
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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