CVE-2016-6433

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

Summary

CVE	CVE-2016-6433
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-10-06 10:59:14 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The Threat Management Console in Cisco Firepower Management Center 5.2.0 through 6.0.1 allows remote authenticated

Risk And Classification

Primary CVSS: v3.1 8.8 HIGH from nvd@nist.gov

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.696560000 probability, percentile 0.986770000 (date 2026-05-07)

Problem Types: CWE-20 | n/a

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	9		AV:N/AC:L/Au:S/C:C/I:C/A:C

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

Single

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Secure Firewall Management Center	5.2.0	All	All	All
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	6.0.1	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 Firepower Management Center CVE-2016-6433 Remote Command Execution Vulnerability	af854a3a-2127-422b-91ae-36
Cisco Firepower Management Console 6.0 Post Authentication UserAdd ≈ Packet Storm	af854a3a-2127-422b-91ae-36
Cisco Firepower Threat Management Console Remote Command Execution Vulnerability	af854a3a-2127-422b-91ae-36
Cisco Firepower Threat Management Console 6.0.1 - Remote Command Execution - CGI webapps Exploit	af854a3a-2127-422b-91ae-36
KoreBlog virtual_appliance_spelunking	af854a3a-2127-422b-91ae-36
www.korelogic.com/Resources/Advisories/KL-001-2016-007.txt	af854a3a-2127-422b-91ae-36
Cisco Firepower Management Console 6.0 - Post Authentication UserAdd (Metasploit) - Linux remote Exploit	af854a3a-2127-422b-91ae-36
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.