CVE-2015-6357

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

Summary

CVE	CVE-2015-6357
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-11-18 11:59:01 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The rule-update feature in Cisco FireSIGHT Management Center (MC) 5.2 through 5.4.0.1 does not verify the X.509 certific

Risk And Classification

Primary CVSS: v2.0 6.8 from nvd@nist.gov

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

Problem Types: CWE-20 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Firesight System Software	5.2.0	All	All	All

Application	Cisco	Firesight System Software	5.3.0	All	All	All
Application	Cisco	Firesight System Software	5.3.1.1	All	All	All
Application	Cisco	Firesight System Software	5.3.1.2	All	All	All
Application	Cisco	Firesight System Software	5.3.1.5	All	All	All
Application	Cisco	Firesight System Software	5.4.0	All	All	All
Application	Cisco	Firesight System Software	5.4.0.1	All	All	All

Vendor Declared Affected Products

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

References

Reference
Wad of Stuff: CVE-2015-6357: FirePWNER Exploit for Cisco FireSIGHT Management Center SSL Validation Vulnerability
Cisco FireSIGHT Management Center Certificate Validation Vulnerability
Cisco FireSIGHT Management Center Certificate Validation ≈ Packet Storm
Cisco FireSIGHT Management Center SSL Validation Flaw Lets Remote Users Execute Arbitrary Code on the Target System - SecurityTracke
Full Disclosure: CVE-2015-6357: Cisco FireSIGHT Management Center SSL Validation Vulnerability
SecurityFocus
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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