



CVE-2019-1931

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2019-1931
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-07-06 02:15:00 UTC
Updated	2019-10-09 23:48:00 UTC
Description	Multiple vulnerabilities in the RSS dashboard in the web-based management interface of Cisco Firepower Management Center (FMC) versions 6.2.3 through 6.5.0. An attacker with access to the FMC web interface can exploit these vulnerabilities to execute arbitrary code on the FMC. The vulnerabilities are related to the RSS feed functionality and involve a cross-site scripting (XSS) attack. The attack is performed by sending a specially crafted RSS feed to the FMC, which then renders the feed in the web interface. The attacker can then inject malicious code into the feed, which is executed by the browser. The vulnerabilities are considered high severity because they allow an attacker to execute arbitrary code on the FMC, which could lead to a complete compromise of the system. The vulnerabilities are patched in FMC versions 6.2.3(1), 6.3.0(1), 6.4.0(1), and 6.5.0(1).

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Firepower Management Center	6.2.3	All	All	All
Application	Cisco	Firepower Management Center	6.3.0	All	All	All
Application	Cisco	Firepower Management Center	6.4.0	All	All	All
Application	Cisco	Firepower Management Center	6.5.0	All	All	All
Application	Cisco	Firepower Management Center	6.2.3	All	All	All
Application	Cisco	Firepower Management Center	6.3.0	All	All	All
Application	Cisco	Firepower Management Center	6.4.0	All	All	All
Application	Cisco	Firepower Management Center	6.5.0	All	All	All

References

Reference	Source	Link	Tags
Cisco Firepower Management Center RSS Cross-Site Scripting Vulnerabilities	CISCO	tools.cisco.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)