Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software SAML Reflected Cross-Site Scripting Vulnerability

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

Summary

CVE	CVE-2026-20102
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-04 18:16:25 UTC
Updated	2026-04-16 20:28:09 UTC
Description	A vulnerability in the SAML 2.0 single sign-on (SSO) feature of Cisco Secure Firewall ASA Software and Cisco Secure Firev

Risk And Classification

Primary CVSS: v3.1 6.1 MEDIUM from psirt@cisco.com

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

Problem Types: CWE-79 | CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
3.1	psirt@cisco.com	Primary	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
3.1	CNA	CVSSV3_1	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

Low

ntegrity

Low

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Adaptive Security Appliance Software	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.16.1	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.16.1.28	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.16.2	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.16.2.3	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.16.2.7	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.17.1	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.16.2.11	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.16.2.13	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.16.2.14	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.17.1.7	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.17.1.9	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.17.1.10	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.17.1.11	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.17.1.13	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.17.1.15	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.17.1.20	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.17.1.30	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.17.1.33	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.17.1.39	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.17.1.45	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.17.1.46	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.23.1.13	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.20.4.7	Not specified

CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.22.2.13	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.18.4.66	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.20.4.10	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.23.1.19	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.18.4.67	Not specified
CNA	Cisco	Cisco Secure Firewall Threat Defense FTD Software	affected 7.0.0	Not specified
CNA	Cisco	Cisco Secure Firewall Threat Defense FTD Software	affected 7.0.0.1	Not specified
CNA	Cisco	Cisco Secure Firewall Threat Defense FTD Software	affected 7.0.1	Not specified
CNA	Cisco	Cisco Secure Firewall Threat Defense FTD Software	affected 7.1.0	Not specified
CNA	Cisco	Cisco Secure Firewall Threat Defense FTD Software	affected 7.0.1.1	Not specified
CNA	Cisco	Cisco Secure Firewall Threat Defense FTD Software	affected 7.1.0.1	Not specified
CNA	Cisco	Cisco Secure Firewall Threat Defense FTD Software	affected 7.1.0.2	Not specified
CNA	Cisco	Cisco Secure Firewall Threat Defense FTD Software	affected 7.1.0.3	Not specified

References

Reference	Source	Link	Ta
sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd...	psirt@cisco.com	sec.cloudapps.cisco.com	Ve
CVE Program record	CVE.ORG	www.cve.org	car
NVD vulnerability detail	NVD	nvd.nist.gov	car

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Exploits

CNA: The Cisco Product Security Incident Response Team (PSIRT) is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

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