



# CVE-2026-20014

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

## Summary

<b>CVE</b>	CVE-2026-20014
<b>State</b>	PUBLISHED
<b>Assigner</b>	cisco
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-04 18:16:15 UTC
<b>Updated</b>	2026-04-16 20:11:34 UTC
<b>Description</b>	A vulnerability in the IKEv2 feature of Cisco Secure Firewall ASA Software and Cisco Secure FTD Software could allow an

## Risk And Classification

**Primary CVSS:** v3.1 7.7 HIGH from psirt@cisco.com

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

**Problem Types:** CWE-401 | CWE-401 Missing Release of Memory after Effective Lifetime

Version	Source	Type	Score	Severity	Vector
3.1	psirt@cisco.com	Primary	7.7	HIGH	<b>CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H</b>
3.1	CNA	CVSSV3_1	7.7	HIGH	<b>CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H</b>

## CVSS v3.1 Breakdown

Attack Vector

**Network**

Attack Complexity

**Low**

Privileges Required

**Low**

User Interaction

**None**

Scope

**Changed**

Confidentiality

**None**

Integrity

**None**

Availability

High

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

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 9.18.1	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.18.1.3	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.18.2	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.18.2.5	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.18.2.7	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.18.2.8	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.18.3	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.18.3.39	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.18.3.46	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.18.3.53	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.18.3.55	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.18.3.56	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.18.4	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.18.4.5	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.18.4.8	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.18.4.22	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.18.4.24	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.18.4.29	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.18.4.34	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.18.4.40	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.18.4.47	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.18.4.50	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.18.4.52	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.18.4.53	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.18.4.57	Not specified
CNA	Cisco	Cisco Secure Firewall Adaptive Security Appliance ASA Software	affected 9.18.4.66	Not specified





CNA	Cisco	<a href="#">Cisco Secure Firewall Threat Defense FTD Software</a>	affected 7.6.0	Not specified
CNA	Cisco	<a href="#">Cisco Secure Firewall Threat Defense FTD Software</a>	affected 7.6.1	Not specified
CNA	Cisco	<a href="#">Cisco Secure Firewall Threat Defense FTD Software</a>	affected 7.6.2	Not specified
CNA	Cisco	<a href="#">Cisco Secure Firewall Threat Defense FTD Software</a>	affected 7.6.2.1	Not specified
CNA	Cisco	<a href="#">Cisco Secure Firewall Threat Defense FTD Software</a>	affected 7.7.0	Not specified
CNA	Cisco	<a href="#">Cisco Secure Firewall Threat Defense FTD Software</a>	affected 7.7.10	Not specified
CNA	Cisco	<a href="#">Cisco Secure Firewall Threat Defense FTD Software</a>	affected 7.7.10.1	Not specified

## References

Reference	Source	Link	Tags
<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd...">sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd...</a>	psirt@cisco.com	<a href="https://sec.cloudapps.cisco.com">sec.cloudapps.cisco.com</a>	Vendor
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	Canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	Canonical

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 vulnerabilities that are described in this advisory.

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](#).

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)