



# CVE-2020-3452

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2020-3452
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@cisco.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-07-22 20:15:00 UTC
<b>Updated</b>	2023-11-07 03:22:00 UTC
<b>Description</b>	A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat

## Risk And Classification

**EPSS:** 0.944520000 probability, percentile 0.999910000 (date 2026-04-22)

**CISA KEV:** Listed on 2021-11-03; due 2022-05-03; ransomware use Unknown

**Problem Types:** CWE-22

## CISA Known Exploited Vulnerability

<b>Vendor</b>	Cisco
<b>Product</b>	Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD)
<b>Name</b>	Cisco ASA and FTD Read-Only Path Traversal Vulnerability
<b>Required Action</b>	Apply updates per vendor instructions.
<b>Notes</b>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2020-3452">https://nvd.nist.gov/vuln/detail/CVE-2020-3452</a>

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Cisco</a>	<a href="#">Adaptive Security Appliance</a>	All	All	All	All
Application	<a href="#">Cisco</a>	<a href="#">Adaptive Security Appliance</a>	All	All	All	All
Operating System	<a href="#">Cisco</a>	<a href="#">Adaptive Security Appliance Software</a>	All	All	All	All
Hardware	<a href="#">Cisco</a>	<a href="#">Asa 5505</a>	-	All	All	All
Hardware	<a href="#">Cisco</a>	<a href="#">Asa 5505</a>	-	All	All	All
Hardware	<a href="#">Cisco</a>	<a href="#">Asa 5510</a>	-	All	All	All
Hardware	<a href="#">Cisco</a>	<a href="#">Asa 5510</a>	-	All	All	All
Hardware	<a href="#">Cisco</a>	<a href="#">Asa 5512-x</a>	-	All	All	All

Hardware	Cisco	Asa 5512-x	-	All	All	All
Hardware	Cisco	Asa 5515-x	-	All	All	All
Hardware	Cisco	Asa 5515-x	-	All	All	All
Hardware	Cisco	Asa 5520	-	All	All	All
Hardware	Cisco	Asa 5520	-	All	All	All
Hardware	Cisco	Asa 5525-x	-	All	All	All
Hardware	Cisco	Asa 5525-x	-	All	All	All
Hardware	Cisco	Asa 5540	-	All	All	All
Hardware	Cisco	Asa 5540	-	All	All	All
Hardware	Cisco	Asa 5545-x	-	All	All	All
Hardware	Cisco	Asa 5545-x	-	All	All	All
Hardware	Cisco	Asa 5550	-	All	All	All
Hardware	Cisco	Asa 5550	-	All	All	All
Hardware	Cisco	Asa 5555-x	-	All	All	All
Hardware	Cisco	Asa 5555-x	-	All	All	All
Hardware	Cisco	Asa 5580	-	All	All	All
Hardware	Cisco	Asa 5580	-	All	All	All
Hardware	Cisco	Asa 5585-x	-	All	All	All
Hardware	Cisco	Asa 5585-x	-	All	All	All
Application	Cisco	Firepower Threat Defense	All	All	All	All
Application	Cisco	Firepower Threat Defense	All	All	All	All

## References

### Reference

Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Web Services Read-Only Path Traversal Vulnerability

Cisco ASA / FTD Remote File Disclosure ≈ Packet Storm

Cisco Adaptive Security Appliance Software 9.11 Local File Inclusion ≈ Packet Storm

Cisco ASA / FTD 9.6.4.42 Path Traversal ≈ Packet Storm

Cisco ASA 9.14.1.10 / FTD 6.6.0.1 Path Traversal ≈ Packet Storm

CVE Program record

NVD vulnerability detail

CISA Known Exploited Vulnerabilities catalog



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](#).

**Free CVE JSON API** [cve.report/api](#)

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