

# CVE-2020-3452

## Cisco ASA and FTD Read-Only Path Traversal Vulnerability

CISA KEV since Nov 3, 2021

Actively exploited

A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct directory traversal attacks and read sensitive files on a targeted system. The vulnerability is due to a lack of proper input validation of URLs in HTTP requests processed by an affected device.

|                                                                |                                                      |                                                                   |                                                                                           |
|----------------------------------------------------------------|------------------------------------------------------|-------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| <p>EVRS</p> <p><b>84</b>/100</p> <p><b>Urgent</b> priority</p> | <p>CVSS V3.1</p> <p><b>7.5</b></p> <p>High · NVD</p> | <p>EPSS</p> <p><b>0.999</b></p> <p>99.99th percentile · FIRST</p> | <p>CISA DEADLINE</p> <p><b>May 3, 2022</b></p> <p>KEV since 2021 · listed over a year</p> |
|----------------------------------------------------------------|------------------------------------------------------|-------------------------------------------------------------------|-------------------------------------------------------------------------------------------|

### Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

|                                                     |                                          |                                                                |                                            |
|-----------------------------------------------------|------------------------------------------|----------------------------------------------------------------|--------------------------------------------|
| <input checked="" type="checkbox"/> <b>CISA KEV</b> | Listed in the catalog                    | <input type="checkbox"/> <b>Vendor exploitation</b>            | Confirmed exploitation in the wild         |
| <input type="checkbox"/> <b>Ransomware</b>          | No known ransomware campaign association | <input type="checkbox"/> <b>KEV recency</b>                    | On the CISA KEV catalog for over two years |
| <input checked="" type="checkbox"/> <b>EPSS</b>     | 0.999 probability                        | <input type="checkbox"/> <b>Pre-patch disclosure</b>           | Disclosure status unavailable              |
| <input checked="" type="checkbox"/> <b>CVSS</b>     | Base score 7.5                           | <input type="checkbox"/> <b>Microsoft Exploitability Index</b> | Not a Microsoft CVE                        |

### Remediation

**Patch This Cycle** Patch or fixed version identified

**CISA required action:** Apply updates per vendor instructions.

Basis: CISA KEV required action

An attacker could exploit this vulnerability by sending a crafted HTTP request containing directory traversal character sequences to an affected device. A successful exploit could allow the attacker to view arbitrary files within the web services file system on the targeted device. The web services file system is enabled when the affected device is configured with either WebVPN or AnyConnect features. This vulnerability cannot be used to obtain access to ASA or FTD system files or underlying operating system (OS) files.

### Affected and fixed versions · 6 more affected products on the NVD record

| PACKAGE                              | AFFECTED                                                                                                                                                                            | FIXED IN                                                                 | SOURCE |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|--------|
| secure firewall threat defense       | $\geq 6.2.3 < 6.2.3.16$<br>$\geq 6.3.0 < 6.3.0.6$<br>$\geq 6.4.0 < 6.4.0.10$<br>$\geq 6.5.0 < 6.5.0.5$<br>$\geq 6.6.0 < 6.6.0.1$                                                    | no fixed version listed                                                  | NVD    |
| adaptive security appliance software | $\geq 9.6 < 9.6.4.42$<br>$\geq 9.8 < 9.8.4.20$<br>$\geq 9.9 < 9.9.2.74$<br>$\geq 9.10 < 9.10.1.42$<br>$\geq 9.12 < 9.12.3.12$<br>$\geq 9.13 < 9.13.1.10$<br>$\geq 9.14 < 9.14.1.10$ | 9.6.4.42 · 9.8.4.20 ·<br>9.9.2.74 · 9.10.1.42 ·<br>9.12.3.12 · 9.13.1.10 | NVD    |
| asa 5505                             | —                                                                                                                                                                                   | no fixed version listed                                                  | NVD    |
| asa 5510                             | —                                                                                                                                                                                   | no fixed version listed                                                  | NVD    |
| asa 5512-x                           | —                                                                                                                                                                                   | no fixed version listed                                                  | NVD    |

| PACKAGE    | AFFECTED | FIXED IN                | SOURCE |
|------------|----------|-------------------------|--------|
| asa 5515-x | –        | no fixed version listed | NVD    |
| asa 5520   | –        | no fixed version listed | NVD    |
| asa 5525-x | –        | no fixed version listed | NVD    |

## Sources

|                        |                                                                                                                                                                                                                     |                   |                                                                                                                         |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>Vendor guidance</b> | <a href="https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafth-ro-path-KJuQhB86">tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafth-ro-path-KJuQhB86</a> | <b>NVD</b>        | <a href="https://nvd.nist.gov/vuln/detail/CVE-2020-3452">nvd.nist.gov/vuln/detail/CVE-2020-3452</a>                     |
| <b>CISA KEV</b>        | <a href="https://cisa.gov/known-exploited-vulnerabilities-catalog">cisa.gov/known-exploited-vulnerabilities-catalog</a>                                                                                             | <b>ENISA EUVD</b> | <a href="https://europa.eu/enisa/eu-vulnerability/EUVD-2020-24723">europa.eu/enisa/eu-vulnerability/EUVD-2020-24723</a> |
| <b>Current data</b>    | <a href="https://evulnable.com/vulnerability-management/cve/CVE-2020-3452">evulnable.com/vulnerability-management/cve/CVE-2020-3452</a>                                                                             |                   |                                                                                                                         |

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.