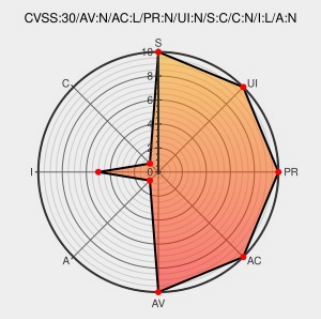
# CVE-2020-3564

Published on: 10/21/2020 12:00:00 AM UTC

Last Modified on: 08/16/2023 04:17:00 PM UTC

## CVE-2020-3564 - advisory for cisco-sa-asaftd-ftpbypass-HY3UTxYu

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF




Certain versions of Adaptive Security Appliance from Cisco contain the following vulnerability:

A vulnerability in the FTP inspection engine of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass FTP inspection. The vulnerability is due to ineffective flow tracking of FTP traffic. An attacker could exploit this vulnerability by sending crafted FTP traffic through an affected device. A successful exploit could allow the attacker to bypass FTP inspection and successfully complete FTP connections.

CVE-2020-3564 has been assigned by psirt@cisco.com to track the vulnerability - currently rated as MEDIUM severity.

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.

Affected Vendor/Software: **Cisco** - **Cisco Adaptive Security Appliance (ASA) Software** version **n/a**

### CVSS3 Score: 5.3 - MEDIUM

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|---|---|---|---|
| NETWORK | LOW | NONE | NONE |
| **Scope** | **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| UNCHANGED | NONE | LOW | NONE |

### CVSS2 Score: 5 - MEDIUM

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | LOW | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| NONE | PARTIAL | NONE |

## CVE References

| Description | Tags | Link |
|---|---|---|
| Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software FTP Inspection Bypass Vulnerability | Vendor Advisory<br>tools.cisco.com<br>text/html | CISCO 20201021 Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software FTP Inspection Bypass Vulnerability |



There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Cisco | Adaptive Security Appliance | All | All | All | All |
| Application | Cisco | Adaptive Security Appliance | All | All | All | All |
| Operating System | Cisco | Adaptive Security Appliance Software | All | All | All | All |
| Application | Cisco | Firepower Threat Defense | All | All | All | All |
| Application | Cisco | Firepower Threat Defense | All | All | All | All |

cpe:2.3:a:cisco:adaptive_security_appliance:*:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:adaptive_security_appliance:*:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:adaptive_security_appliance_software:*:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:firepower_threat_defense:*:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:firepower_threat_defense:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

## Social Mentions

| Source | Title | Posted (UTC) |
|---|---|---|

← Previous ID

Next ID→

**CVE.report and Source URL Uptime Status status.cve.report**