



CVE-2012-0355

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

| | |
|------------------------|---|
| CVE | CVE-2012-0355 |
| State | PUBLIC |
| Assigner | psirt@cisco.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2012-03-15 00:55:00 UTC |
| Updated | 2023-08-15 14:41:00 UTC |
| Description | Cisco Adaptive Security Appliances (ASA) 5500 series devices, and the ASA Services Module (ASASM) in Cisco Catalyst 6 |

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|--------|---|-----------|--------|---------|----------|
| Hardware | Cisco | 5500 Series Adaptive Security Appliance | All | All | All | All |
| Hardware | Cisco | 5500 Series Adaptive Security Appliance | All | All | All | All |
| Application | Cisco | Adaptive Security Appliance Software | 8.4 | All | All | All |
| Application | Cisco | Adaptive Security Appliance Software | 8.4(1) | All | All | All |
| Application | Cisco | Adaptive Security Appliance Software | 8.4(1.11) | All | All | All |
| Application | Cisco | Adaptive Security Appliance Software | 8.4(2) | All | All | All |
| Application | Cisco | Adaptive Security Appliance Software | 8.4(2.11) | All | All | All |
| Application | Cisco | Adaptive Security Appliance Software | 8.4\1.11\ | All | All | All |
| Application | Cisco | Adaptive Security Appliance Software | 8.4\1\ | All | All | All |
| Application | Cisco | Adaptive Security Appliance Software | 8.4\2.11\ | All | All | All |
| Application | Cisco | Adaptive Security Appliance Software | 8.4\2\ | All | All | All |
| Application | Cisco | Adaptive Security Appliance Software | 8.5 | All | All | All |
| Application | Cisco | Adaptive Security Appliance Software | 8.5(1) | All | All | All |
| Application | Cisco | Adaptive Security Appliance Software | 8.5(1.4) | All | All | All |
| Application | Cisco | Adaptive Security Appliance Software | 8.5\1.4\ | All | All | All |
| Application | Cisco | Adaptive Security Appliance Software | 8.5\1\ | All | All | All |
| Operating System | Cisco | Adaptive Security Appliance Software | 8.4 | All | All | All |

| | | | | | | |
|------------------|-------|--|-----------|-----|-----|-----|
| Operating System | Cisco | Adaptive Security Appliance Software | 8.4\1.11\ | All | All | All |
| Operating System | Cisco | Adaptive Security Appliance Software | 8.4\1\ | All | All | All |
| Operating System | Cisco | Adaptive Security Appliance Software | 8.4\2.11\ | All | All | All |
| Operating System | Cisco | Adaptive Security Appliance Software | 8.4\2\ | All | All | All |
| Operating System | Cisco | Adaptive Security Appliance Software | 8.5 | All | All | All |
| Operating System | Cisco | Adaptive Security Appliance Software | 8.5\1.4\ | All | All | All |
| Operating System | Cisco | Adaptive Security Appliance Software | 8.5\1\ | All | All | All |
| Application | Cisco | Adaptive Security Appliance Software | 8.4 | All | All | All |
| Application | Cisco | Adaptive Security Appliance Software | 8.4\1.11\ | All | All | All |
| Application | Cisco | Adaptive Security Appliance Software | 8.4\1\ | All | All | All |
| Application | Cisco | Adaptive Security Appliance Software | 8.4\2.11\ | All | All | All |
| Application | Cisco | Adaptive Security Appliance Software | 8.4\2\ | All | All | All |
| Application | Cisco | Adaptive Security Appliance Software | 8.5 | All | All | All |
| Application | Cisco | Adaptive Security Appliance Software | 8.5\1.4\ | All | All | All |
| Application | Cisco | Adaptive Security Appliance Software | 8.5\1\ | All | All | All |
| Hardware | Cisco | Catalyst 6500 | All | All | All | All |
| Hardware | Cisco | Catalyst 6500 | All | All | All | All |
| Hardware | Cisco | Catalyst 6503-e | - | All | All | All |
| Hardware | Cisco | Catalyst 6503-e | - | All | All | All |
| Hardware | Cisco | Catalyst 6504-e | - | All | All | All |
| Hardware | Cisco | Catalyst 6504-e | - | All | All | All |
| Hardware | Cisco | Catalyst 6506-e | - | All | All | All |
| Hardware | Cisco | Catalyst 6506-e | - | All | All | All |
| Hardware | Cisco | Catalyst 6509-e | - | All | All | All |
| Hardware | Cisco | Catalyst 6509-e | - | All | All | All |
| Hardware | Cisco | Catalyst 6509-neb-a | - | All | All | All |
| Hardware | Cisco | Catalyst 6509-neb-a | - | All | All | All |
| Hardware | Cisco | Catalyst 6509-v-e | - | All | All | All |
| Hardware | Cisco | Catalyst 6509-v-e | - | All | All | All |
| Hardware | Cisco | Catalyst 6513 | - | All | All | All |
| Hardware | Cisco | Catalyst 6513 | - | All | All | All |
| Hardware | Cisco | Catalyst 6513-e | - | All | All | All |
| Hardware | Cisco | Catalyst 6513-e | - | All | All | All |

References

Reference

Cisco ASA Multiple Bugs Let Remote Users Deny Service - SecurityTracker

Cisco Security Advisory: Multiple Vulnerabilities in Cisco ASA 5500 Series Adaptive Security Appliances and Cisco Catalyst 6500 Series ASA

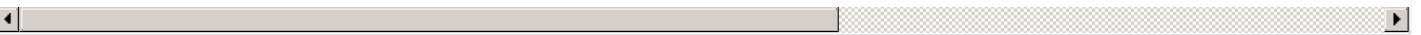
Security Advisory SA48423 - Cisco Adaptive Security Appliances Multiple Denial of Service Vulnerabilities - Secunia

Cisco ASA Syslog Message 305006 Denial of Service Vulnerability

80045

CVE Program record

NVD vulnerability detail



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](#).

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