



CVE-2010-0151

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2010-0151 |
| State | PUBLIC |
| Assigner | psirt@cisco.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2010-02-19 17:30:00 UTC |
| Updated | 2017-08-17 01:31:00 UTC |
| Description | The Cisco Firewall Services Module (FWSM) 4.0 before 4.0(8), as used in for the Cisco Catalyst 6500 switches, Cisco 7600 |

Risk And Classification

Problem Types: NVD-CWE-Other

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 |
| Hardware | Cisco | 5505 Series Adaptive Security Appliance | All | All | All | All |
| Hardware | Cisco | 5505 Series Adaptive Security Appliance | All | All | All | All |
| Hardware | Cisco | 5510 Series Adaptive Security Appliance | All | All | All | All |
| Hardware | Cisco | 5510 Series Adaptive Security Appliance | All | All | All | All |
| Hardware | Cisco | 5520 Series Adaptive Security Appliance | All | All | All | All |
| Hardware | Cisco | 5520 Series Adaptive Security Appliance | All | All | All | All |
| Hardware | Cisco | 5540 Series Adaptive Security Appliance | All | All | All | All |
| Hardware | Cisco | 5540 Series Adaptive Security Appliance | All | All | All | All |
| Hardware | Cisco | 5550 Series Adaptive Security Appliance | All | All | All | All |
| Hardware | Cisco | 5550 Series Adaptive Security Appliance | All | All | All | All |
| Hardware | Cisco | 5580 Series Adaptive Security Appliance | All | All | All | All |
| Hardware | Cisco | 5580 Series Adaptive Security Appliance | All | All | All | All |
| Hardware | Cisco | Asa 5500 | All | All | All | All |
| Hardware | Cisco | Asa 5500 | All | All | All | All |
| Hardware | Cisco | Catalyst 6500 | All | All | All | All |

| | | | | | | |
|----------|-------|--------------------------|--------|-----|-----|-----|
| Hardware | Cisco | Catalyst 6500 | All | All | All | All |
| Hardware | Cisco | Catalyst 7600 | All | All | All | All |
| Hardware | Cisco | Catalyst 7600 | All | All | All | All |
| Hardware | Cisco | Firewall Services Module | 4.0 | All | All | All |
| Hardware | Cisco | Firewall Services Module | 4.0(4) | All | All | All |
| Hardware | Cisco | Firewall Services Module | 4.0(6) | All | All | All |
| Hardware | Cisco | Firewall Services Module | 4.0(4) | All | All | All |
| Hardware | Cisco | Firewall Services Module | 4.0(6) | All | All | All |
| Hardware | Cisco | Firewall Services Module | 4.0 | All | All | All |
| Hardware | Cisco | Firewall Services Module | 4.0(4) | All | All | All |
| Hardware | Cisco | Firewall Services Module | 4.0(6) | All | All | All |

References

Reference

Cisco Security Advisory: Cisco Firewall Services Module Skinny Client Control Protocol Inspection Denial of Service Vulnerability - Cisco Systems

Cisco Firewall Services Module Denial of Service Vulnerability - Advisories - Community

Cisco Security Advisory: Multiple Vulnerabilities in Cisco ASA 5500 Series Adaptive Security Appliances - Cisco Systems

62432

Cisco Firewall Services Module SCCP Inspection Remote Denial of Service Vulnerability

IBM X-Force Exchange

Cisco Firewall Services Module SCCP Protocol Flaw Lets Remote Users Deny Service - SecurityTracker

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

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](#)