



CVE-2018-0240

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

Summary

CVE	CVE-2018-0240
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-04-19 20:29:00 UTC
Updated	2023-08-15 15:24:00 UTC
Description	Multiple vulnerabilities in the Application Layer Protocol Inspection feature of Cisco Adaptive Security Appliance (ASA) Soft

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	7604	-	All	All	All
Hardware	Cisco	7604	-	All	All	All
Hardware	Cisco	7606-s	-	All	All	All
Hardware	Cisco	7606-s	-	All	All	All
Hardware	Cisco	7609-s	-	All	All	All
Hardware	Cisco	7609-s	-	All	All	All
Hardware	Cisco	7613-s	-	All	All	All
Hardware	Cisco	7613-s	-	All	All	All
Application	Cisco	Adaptive Security Appliance Software	All	All	All	All
Application	Cisco	Adaptive Security Appliance Software	101.3(1.23)	All	All	All
Application	Cisco	Adaptive Security Appliance Software	101.3(1.51)	All	All	All
Application	Cisco	Adaptive Security Appliance Software	101.3\1.23\	All	All	All
Application	Cisco	Adaptive Security Appliance Software	101.3\1.51\	All	All	All
Application	Cisco	Adaptive Security Appliance Software	101.4(1.24)	All	All	All
Application	Cisco	Adaptive Security Appliance Software	101.4\1.24\	All	All	All
Application	Cisco	Adaptive Security Appliance Software	9.6(4)	All	All	All
Application	Cisco	Adaptive Security Appliance Software	9.6(4\)	All	All	All

Application	Cisco	Adaptive Security Appliance Software	9.7(1)	All	All	All
Application	Cisco	Adaptive Security Appliance Software	9.7(1.17)	All	All	All
Application	Cisco	Adaptive Security Appliance Software	9.7(1.17\)	All	All	All
Application	Cisco	Adaptive Security Appliance Software	9.7(1\)	All	All	All
Application	Cisco	Adaptive Security Appliance Software	9.8(2.12)	All	All	All
Application	Cisco	Adaptive Security Appliance Software	9.8(2.21)	All	All	All
Application	Cisco	Adaptive Security Appliance Software	9.8(2.12\)	All	All	All
Application	Cisco	Adaptive Security Appliance Software	9.8(2.21\)	All	All	All
Application	Cisco	Adaptive Security Appliance Software	9.9(1.77)	All	All	All
Application	Cisco	Adaptive Security Appliance Software	9.9(1.77\)	All	All	All
Application	Cisco	Adaptive Security Appliance Software	99.1(20.190)	All	All	All
Application	Cisco	Adaptive Security Appliance Software	99.1(20.190\)	All	All	All
Application	Cisco	Adaptive Security Appliance Software	99.2(0.32)	All	All	All
Application	Cisco	Adaptive Security Appliance Software	99.2(0.32\)	All	All	All
Operating System	Cisco	Adaptive Security Appliance Software	All	All	All	All
Application	Cisco	Adaptive Security Appliance Software	All	All	All	All
Application	Cisco	Adaptive Security Appliance Software	101.3(1.23\)	All	All	All
Application	Cisco	Adaptive Security Appliance Software	101.3(1.51\)	All	All	All
Application	Cisco	Adaptive Security Appliance Software	101.4(1.24\)	All	All	All
Application	Cisco	Adaptive Security Appliance Software	9.6(4\)	All	All	All
Application	Cisco	Adaptive Security Appliance Software	9.7(1.17\)	All	All	All
Application	Cisco	Adaptive Security Appliance Software	9.7(1\)	All	All	All
Application	Cisco	Adaptive Security Appliance Software	9.8(2.12\)	All	All	All
Application	Cisco	Adaptive Security Appliance Software	9.8(2.21\)	All	All	All
Application	Cisco	Adaptive Security Appliance Software	9.9(1.77\)	All	All	All
Application	Cisco	Adaptive Security Appliance Software	99.1(20.190\)	All	All	All
Application	Cisco	Adaptive Security Appliance Software	99.2(0.32\)	All	All	All
Application	Cisco	Adaptive Security Virtual Appliance	-	All	All	All
Application	Cisco	Adaptive Security Virtual Appliance	v10	All	All	All
Application	Cisco	Adaptive Security Virtual Appliance	v30	All	All	All
Application	Cisco	Adaptive Security Virtual Appliance	v5	All	All	All
Application	Cisco	Adaptive Security Virtual Appliance	v50	All	All	All
Application	Cisco	Adaptive Security Virtual Appliance	v10	All	All	All
Application	Cisco	Adaptive Security Virtual Appliance	v30	All	All	All
Application	Cisco	Adaptive Security Virtual Appliance	v5	All	All	All

Application	Cisco	Adaptive Security Virtual Appliance	v50	All	All	All
Hardware	Cisco	Asa-5505	-	All	All	All
Hardware	Cisco	Asa-5505	-	All	All	All
Hardware	Cisco	Asa-5506-x	-	All	All	All
Hardware	Cisco	Asa-5506-x	-	All	All	All
Hardware	Cisco	Asa-5506h-x	-	All	All	All
Hardware	Cisco	Asa-5506h-x	-	All	All	All
Hardware	Cisco	Asa-5512-x	-	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-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-5555-x	-	All	All	All
Hardware	Cisco	Asa-5555-x	-	All	All	All
Hardware	Cisco	Asa-5585-x	-	All	All	All
Hardware	Cisco	Asa-5585-x	-	All	All	All
Hardware	Cisco	Asa 5506-x	-	All	All	All
Hardware	Cisco	Asa 5506-x	-	All	All	All
Hardware	Cisco	Asa 5506w-x	-	All	All	All
Hardware	Cisco	Asa 5506w-x	-	All	All	All
Hardware	Cisco	Asa 5508-x	-	All	All	All
Hardware	Cisco	Asa 5508-x	-	All	All	All
Hardware	Cisco	Asa 5510	-	All	All	All
Hardware	Cisco	Asa 5510	-	All	All	All
Hardware	Cisco	Asa 5516-x	-	All	All	All
Hardware	Cisco	Asa 5516-x	-	All	All	All
Hardware	Cisco	Asa 5525-x	-	All	All	All
Hardware	Cisco	Asa 5525-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	Catalyst 6500-e	-	All	All	All
Hardware	Cisco	Catalyst 6500-e	-	All	All	All
Hardware	Cisco	Catalyst 6503-e	-	All	All	All
Hardware	Cisco	Catalyst 6504-e	-	All	All	All
Hardware	Cisco	Catalyst 6506-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-v-e	-	All	All	All
Hardware	Cisco	Catalyst 6513	-	All	All	All
Hardware	Cisco	Catalyst 6513-e	-	All	All	All
Hardware	Cisco	Firepower 2110	-	All	All	All
Hardware	Cisco	Firepower 2110	-	All	All	All
Hardware	Cisco	Firepower 2120	-	All	All	All
Hardware	Cisco	Firepower 2120	-	All	All	All
Hardware	Cisco	Firepower 2130	-	All	All	All
Hardware	Cisco	Firepower 2130	-	All	All	All
Hardware	Cisco	Firepower 2140	-	All	All	All
Hardware	Cisco	Firepower 2140	-	All	All	All
Hardware	Cisco	Firepower 4110	-	All	All	All
Hardware	Cisco	Firepower 4110	-	All	All	All
Hardware	Cisco	Firepower 4120	-	All	All	All
Hardware	Cisco	Firepower 4120	-	All	All	All
Hardware	Cisco	Firepower 4140	-	All	All	All
Hardware	Cisco	Firepower 4140	-	All	All	All
Hardware	Cisco	Firepower 4150	-	All	All	All
Hardware	Cisco	Firepower 4150	-	All	All	All
Hardware	Cisco	Firepower 9300	-	All	All	All
Hardware	Cisco	Firepower 9300	-	All	All	All
Application	Cisco	Firepower Threat Defense	All	All	All	All
Application	Cisco	Firepower Threat Defense	All	All	All	All
Application	Cisco	Firepower Threat Defense Virtual	-	All	All	All
Application	Cisco	Firepower Threat Defense Virtual	-	All	All	All

Application	Cisco	Firepower Threat Defense Virtual	-	All	All	All
Hardware	Cisco	Isa-3000-2c2f	-	All	All	All
Hardware	Cisco	Isa-3000-2c2f	-	All	All	All
Hardware	Cisco	Isa-3000-4c	-	All	All	All
Hardware	Cisco	Isa-3000-4c	-	All	All	All

References

Reference	Source
Cisco Adaptive Security Appliance Application Layer Protocol Inspection Denial of Service Vulnerabilities	CONFIRMED
Cisco ASA Application Layer Protocol Inspection Logic Errors Let Remote Users Cause the Target System to Reload - SecurityTracker	SECURITY
Multiple Cisco Products CVE-2018-0240 Multiple Denial of Service Vulnerabilities	BIDEN
Rockwell Automation Allen-Bradley Stratix 5950 CISA	MISPLACED
CVE Program record	CVE
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

590341 Rockwell Automation Allen-Bradley Stratix 5950 Multiple Vulnerabilities (ICSA-18-184-01)

© 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](#)