



CVE-2018-0228

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

Summary

CVE	CVE-2018-0228
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 15:37:00 UTC
Description	A vulnerability in the ingress flow creation functionality of Cisco Adaptive Security Appliance (ASA) could allow an unauther

Risk And Classification

Problem Types: CWE-667

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Adaptive Security Appliance Software	All	All	All	All
Application	Cisco	Adaptive Security Appliance Software	98.1(12.187)	All	All	All
Application	Cisco	Adaptive Security Appliance Software	98.1\12.187)	All	All	All
Operating System	Cisco	Adaptive Security Appliance Software	All	All	All	All
Operating System	Cisco	Adaptive Security Appliance Software	98.1\12.187)	All	All	All
Application	Cisco	Adaptive Security Appliance Software	All	All	All	All
Application	Cisco	Adaptive Security Appliance Software	98.1\12.187)	All	All	All
Application	Cisco	Firepower Threat Defense	All	All	All	All
Application	Cisco	Firepower Threat Defense	All	All	All	All

References

Reference	
Cisco Adaptive Security Appliance (ASA) Software CVE-2018-0228 Denial of Service Vulnerability	S
Cisco Adaptive Security Appliance Flow Creation Denial of Service Vulnerability	E
Cisco ASA Ingress Software Lock Error Lets Remote Users Consume Excessive CPU Resources on the Target System - SecurityTracker	C
Rockwell Automation Allen-Bradley Stratix 5950 CISA	S
CVE Program record	M
	C

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](#)