



CVE-2019-12677

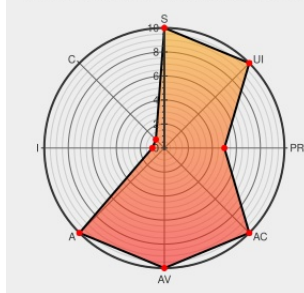
Published on: 10/02/2019 12:00:00 AM UTC

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

CVE-2019-12677 - advisory for cisco-sa-20191002-asa-ssl-vpn-dos

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:30/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H



Certain versions of [Adaptive Security Appliance](#) from [Cisco](#) contain the following vulnerability:

A vulnerability in the Secure Sockets Layer (SSL) VPN feature of Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition that prevents the creation of new SSL/Transport Layer Security (TLS) connections to an affected device. The vulnerability is

due to incorrect handling of Base64-encoded strings. An attacker could exploit this vulnerability by opening many SSL VPN sessions to an affected device. The attacker would need to have valid user credentials on the affected device to exploit this vulnerability. A successful exploit could allow the attacker to overwrite a special system memory location, which will eventually result in memory allocation errors for new SSL/TLS sessions to the device, preventing successful establishment of these sessions. A reload of the device is required to recover from this condition. Established SSL/TLS connections to the device and SSL/TLS connections through the device are not affected. Note: Although this vulnerability is in the SSL VPN feature, successful exploitation of this vulnerability would affect all new SSL/TLS sessions to the device, including management sessions.

CVE-2019-12677 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: **6.5 - MEDIUM**

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

CVSS2 Score: 4 - MEDIUM		
Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Cisco Adaptive Security Appliance Software SSL VPN Denial of Service Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20191002 Cisco Adaptive Security Appliance Software SSL VPN Denial of Service Vulnerability

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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
Application	Cisco	Adaptive Security Appliance Software	All	All	All	All
Operating System	Cisco	Adaptive Security Appliance Software	All	All	All	All
Hardware 	Cisco	Asa 5505	-	All	All	All
Hardware 	Cisco	Asa 5505	-	All	All	All
Hardware 	Cisco	Asa 5510	-	All	All	All
Hardware 	Cisco	Asa 5510	-	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 5525-v	-	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	Asa 5585-x	-	All	All	All
Hardware		Cisco	Asa 5585-x	-	All	All	All
cpe:2.3:a:cisco:adaptive_security_appliance:*****:							
cpe:2.3:a:cisco:adaptive_security_appliance:*****:							
cpe:2.3:a:cisco:adaptive_security_appliance_software:*****:							
cpe:2.3:o:cisco:adaptive_security_appliance_software:*****:							
cpe:2.3:h:cisco:asa_5505:-*****:							
cpe:2.3:h:cisco:asa_5505:-*****:							
cpe:2.3:h:cisco:asa_5510:-*****:							
cpe:2.3:h:cisco:asa_5510:-*****:							
cpe:2.3:h:cisco:asa_5512-x:-*****:							
cpe:2.3:h:cisco:asa_5512-x:-*****:							
cpe:2.3:h:cisco:asa_5515-x:-*****:							
cpe:2.3:h:cisco:asa_5515-x:-*****:							
cpe:2.3:h:cisco:asa_5520:-*****:							
cpe:2.3:h:cisco:asa_5520:-*****:							
cpe:2.3:h:cisco:asa_5525-x:-*****:							
cpe:2.3:h:cisco:asa_5525-x:-*****:							
cpe:2.3:h:cisco:asa_5550:-*****:							
cpe:2.3:h:cisco:asa_5550:-*****:							
cpe:2.3:h:cisco:asa_5555-x:-*****:							
cpe:2.3:h:cisco:asa_5555-x:-*****:							

cpe:2.3:h:cisco:asa_5580:-:*****:
cpe:2.3:h:cisco:asa_5580:-:*****:
cpe:2.3:h:cisco:asa_5585-x:-:*****:
cpe:2.3:h:cisco:asa_5585-x:-:*****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© [CVE.report](#) 2023   |

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](#)