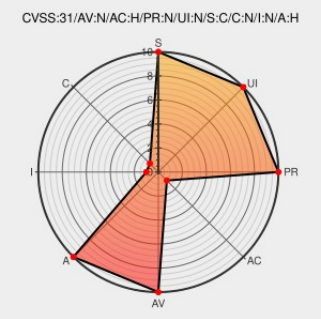
CVE-2018-15397

Published on: 10/05/2018 12:00:00 AM UTC

Last Modified on: 08/15/2023 03:24:00 PM UTC

CVE-2018-15397 - advisory for cisco-sa-20181003-asa-ipsec-dos

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Adaptive Security Appliance Software from Cisco contain the following vulnerability:

A vulnerability in the implementation of Traffic Flow Confidentiality (TFC) over IPsec functionality in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause an affected device to restart unexpectedly, resulting in a denial of service (DoS) condition. The vulnerability is due to an error that may occur if the affected software renegotiates the encryption key for an IPsec tunnel when certain TFC traffic is in flight. An attacker could exploit this vulnerability by sending a malicious stream of TFC traffic through an established IPsec tunnel on an affected device. A successful exploit could allow the attacker to cause a daemon process on the affected device to crash, which could cause the device to crash and result in a DoS condition.

CVE-2018-15397 has been assigned by psirt@cisco.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Cisco** - **Cisco Adaptive Security Appliance (ASA) Software** version **n/a**

CVSS3 Score: 6.8 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	NONE	NONE	HIGH

CVSS2 Score: 7.1 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**

NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
Cisco Adaptive Security Appliance IPsec VPN Denial of Service Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20181003 Cisco Adaptive Security Appliance IPsec VPN Denial of Service Vulnerability
Cisco ASA Traffic Flow Confidentiality Processing Bug Lets Remote Users Cause the Target System to Crash - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTRACK 1041786

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 Software	9.6.4	All	All	All
Application	Cisco	Adaptive Security Appliance Software	9.8.2	All	All	All
Application	Cisco	Adaptive Security Appliance Software	9.9.1	All	All	All
Application	Cisco	Adaptive Security Appliance Software	9.9.1(1)	All	All	All
Application	Cisco	Adaptive Security Appliance Software	9.9.1\(1\)	All	All	All
Operating System	Cisco	Adaptive Security Appliance Software	9.6.4	All	All	All
Operating System	Cisco	Adaptive Security Appliance Software	9.8.2	All	All	All
Operating System	Cisco	Adaptive Security Appliance Software	9.9.1	All	All	All
Operating System	Cisco	Adaptive Security Appliance Software	9.9.1\(1\)	All	All	All
Application	Cisco	Adaptive Security Appliance Software	9.6.4	All	All	All
Application	Cisco	Adaptive Security Appliance Software	9.8.2	All	All	All
Application	Cisco	Adaptive Security Appliance Software	9.9.1	All	All	All
Application	Cisco	Adaptive Security Appliance Software	9.9.1\(1\)	All	All	All
Application	Cisco	Firepower Management Center	6.2.2	All	All	All
Application	Cisco	Firepower Management Center	6.2.2	All	All	All

cpe:2.3:a:cisco:adaptive_security_appliance_software:9.6.4:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:adaptive_security_appliance_software:9.8.2:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:adaptive_security_appliance_software:9.9.1:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:adaptive_security_appliance_software:9.9.1(1):*:*:*:*:*:*:*:

cpe:2.3:a:cisco:adaptive_security_appliance_software:9.9.1\(1\):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:adaptive_security_appliance_software:9.6.4:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:adaptive_security_appliance_software:9.8.2:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:adaptive_security_appliance_software:9.9.1:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:adaptive_security_appliance_software:9.9.1\(1\):*:*:*:*:*:*:*:

cpe:2.3:a:cisco:adaptive_security_appliance_software:9.6.4:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:adaptive_security_appliance_software:9.8.2:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:adaptive_security_appliance_software:9.9.1:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:adaptive_security_appliance_software:9.9.1\(1\):*:*:*:*:*:*:*:

cpe:2.3:a:cisco:firepower_management_center:6.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:firepower_management_center:6.2.2:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→