Cisco Security Advisory

Cisco Adaptive Security Appliance SNMP Remote Code Execution Vulnerability

High

Advisory ID:	cisco-sa-20160817-asa-snmp
Last Updated:	2016 August 25 22:23 GMT
Published:	2016 August 17 18:45 GMT
Version1.4:	Interim
CVSS Score:	Base - 8.5
Workarounds:	Yes
Cisco Bug IDs:	CSCva92151

CVE-2016-6366
CWE-119

Download CVRF

Download PDF

Email

Summary

A vulnerability in the Simple Network Management Protocol (SNMP) code of Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, remote attacker to cause a reload of the affected system or to remotely execute code.

The vulnerability is due to a buffer overflow in the affected code area. The vulnerability affects all versions of SNMP (versions 1, 2c, and 3) when enabled on a virtual or physical Cisco ASA device. An attacker could exploit this vulnerability by sending crafted SNMP packets to an SNMP-enabled interface on the affected system. An exploit could allow the attacker to execute arbitrary code and obtain full control of the system or to cause a reload of the affected system. The attacker must know the SNMP community string to exploit this vulnerability.

Note: Only traffic directed to the affected system can be used to exploit this vulnerability. This vulnerability affects systems configured in routed and transparent firewall mode only and in single or multiple context mode. This vulnerability can be triggered by IPv4 traffic only. The attacker requires knowledge of the configured SNMP community string in SNMP version 1 and SNMP version 2c or a valid username and password for SNMP version 3.

Cisco has released software updates that address this vulnerability. Mitigations are listed in the Workarounds section of this advisory.

This advisory is available at the following link:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-asa-snmp

Affected Products

Vulnerable Products

Affected Cisco ASA Software running on the following products may be affected by this vulnerability:

- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco ASA 5500-X Series Next-Generation Firewalls
- Cisco ASA Services Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers
- Cisco ASA 1000V Cloud Firewall
- Cisco Adaptive Security Virtual Appliance (ASAv)
- Cisco Firepower 4100 Series
- Cisco Firepower 9300 ASA Security Module
- Cisco Firepower Threat Defense Software
- Cisco Firewall Services Module (FWSM)*
- Cisco Industrial Security Appliance 3000
- Cisco PIX Firewalls*

All versions of SNMP are affected by this vulnerability. Refer to the Fixed Software section of this security advisory for more information about the affected releases.

*** Note:** Cisco Firewall Service Modules and Cisco PIX Firewalls have passed the last day of software support milestone as stated in the published End of Life (EoL) documents. Further investigations into these devices will not be performed, and fixed software will not be made available. Please see the following EoL documents for further information:

- Cisco Firewall Services Module (FWSM)
  http://www.cisco.com/c/en/us/products/collateral/interfaces-modules/catalyst-6500-series-firewall-services-module/eol_c51-699134.html
- Cisco PIX Firewalls
  http://www.cisco.com/c/en/us/products/security/pix-500-series-security-appliances/eos-eol-notice-listing.html

Products Confirmed Not Vulnerable

No other Cisco products are currently known to be affected by this vulnerability.

Workarounds

Administrators are advised to allow only trusted users to have SNMP access and to monitor affected systems using the **snmp-server** host command.

The SNMP chapter of the *Cisco ASA Series General Operations CLI Configuration Guide* explains how SNMP is configured in the Cisco ASA.

The attacker must know the community strings to successfully launch an attack against an affected device. Community strings are passwords that are applied to an ASA device to restrict both read-only and read-write access to the SNMP data on the device. These community strings, as with all passwords, should be carefully chosen to ensure they are not trivial. Community strings should be changed at regular intervals and in accordance with network security policies. For example, the strings should be changed when a network administrator changes roles or leaves the company.

Fixed Software

When considering software upgrades, customers are advised to regularly consult the advisories for Cisco products, which are available from the Cisco Security Advisories and Alerts page, to determine exposure and a complete upgrade solution.

In all cases, customers should ensure that the devices to be upgraded contain sufficient memory and confirm that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, customers are advised to contact the Cisco Technical Assistance Center (TAC) or their contracted maintenance providers.

Fixed Releases

Cisco ASA Major Release	First Fixed Release
7.2	Affected; migrate to 9.1.7(9) or later
8.0	Affected; migrate to 9.1.7(9) or later
8.1	Affected; migrate to 9.1.7(9) or later
8.2	Affected; migrate to 9.1.7(9) or later
8.3	Affected; migrate to 9.1.7(9) or later
8.4	Affected; migrate to 9.1.7(9) or later
8.5	Affected; migrate to 9.1.7(9) or later
8.6	Affected; migrate to 9.1.7(9) or later
8.7	Affected; migrate to 9.1.7(9) or later
9.0	9.0.4(40)
9.1	9.1.7(9)
9.2	9.2.4(14)
9.3	9.3.3(10)
9.4	9.4.3(8) ETA 8/26/2016
9.5	9.5(3) ETA 8/30/2016
9.6 (FTD)	9.6.1(11) / FTD 6.0.1(2)
9.6 (ASA)	9.6.2

Exploitation and Public Announcements

On August 15, 2016, Cisco was alerted to information posted online by the Shadow Brokers group, which claimed to possess disclosures from the Equation Group. The posted materials included exploits for firewall products from multiple vendors. The Cisco products mentioned were the Cisco PIX and Cisco ASA firewalls.

Source

The exploit of this vulnerability was publicly disclosed by the alleged Shadow Brokers group.

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-asa-snmp

---

Revision History

Version	Description	Section	Status	Date
1.4	Updated Summary text for additional clarification, updated Fixed Software section to reflect recently published software versions.	Summary, Fixed Software	Interim	2016-August-25

Cisco Security Vulnerability Policy

To learn about Cisco security vulnerability disclosure policies and publications, see the Security Vulnerability Policy. This document also contains instructions for obtaining fixed software and receiving security vulnerability information from Cisco.

Related Resources

ERP Cisco Event Response: Cisco ASA SNMP and CLI Remote Code Execution Vulnerabilities

BLG Shadow Brokers

ST 3:39885

IPS Cisco ASA SNMP Remote Code Execution

Subscribe to Cisco Security Notifications

Subscribe

1.3	Updated Summary text to show updates are available, Fixed Software section with Affected Version and first Fixed Release table.	Summary, Fixed Software	Interim	2016-August-24
1.2	Updated Summary text to match CVSSv2 score (unauthenticated changed to authenticated in text), added clarification to Summary that all versions of SNMP are affected, added new affected products to Affected Products section.	Summary, Affected Products	Interim	2016-August-18
1.1	Cisco has not released software updates that address this vulnerability.	Summary	Interim	2016-August-17
1.0	Initial public release.	-	Interim	2016-August-17
