Cisco Security Advisory

Cisco ASA Software IKEv1 and IKEv2 Buffer Overflow Vulnerability

Critical

Advisory ID:	cisco-sa-20160210-asa-ike
Last Updated:	2016 February 16 23:06 GMT
Published:	2016 February 10 16:00 GMT
Version1.2:	Final
CVSS Score:	Base - 10.0
Workarounds:	No workarounds available
Cisco Bug IDs:	CSCux29978 CSCux42019

CVE-2016-1287
CWE-119

Download CVRF

Download PDF

Email

Summary

A vulnerability in the Internet Key Exchange (IKE) version 1 (v1) and IKE version 2 (v2) code of Cisco ASA Software could allow an unauthenticated, 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. An attacker could exploit this vulnerability by sending crafted UDP packets to 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.

Note: Only traffic directed to the affected system can be used to exploit this vulnerability. This vulnerability affects systems configured in routed firewall mode only and in single or multiple context mode. This vulnerability can be triggered by IPv4 and IPv6 traffic.

Cisco has released software updates that address this vulnerability. This advisory is available at the following link:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160210-asa-ike

Affected 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 9300 ASA Security Module
- Cisco ISA 3000 Industrial Security Appliance

Refer to the "Fixed Software" section of this security advisory for more information about the affected releases.

Vulnerable Products

Cisco ASA Software is affected by this vulnerability if the system is configured to terminate IKEv1 or IKEv2 VPN connections or if configured as an Easy VPN hardware client.

Cisco ASA Software configured to terminate IKEv1 or IKEv2 VPN Connections

Cisco ASA Software is affected by this vulnerability if the system is configured to terminate IKEv1 or IKEv2 VPN connections. This includes the following:

- LAN-to-LAN IPsec VPN
- Remote access VPN using the IPsec VPN client
- Layer 2 Tunneling Protocol (L2TP)-over-IPsec VPN connections
- IKEv2 AnyConnect

Cisco ASA Software is not affected by this vulnerability if the system is configured to terminate only the following VPN connections:

- Clientless SSL
- AnyConnect SSL

To determine whether the Cisco ASA is configured to terminate IKEv1 or IKEv2 VPN connections, a crypto map must be configured for at least one interface. Administrators should use the **show running-config crypto map | include interface** command and verify that it returns output. The following example shows a crypto map called *outside_map* configured on the *outside* interface:

```
ciscoasa# show running-config crypto map | include interface
crypto map outside_map interface outside
```

Note: Due to a misconfiguration or to a partial configuration, the IKEv1 or IKEv2 process may still accept incoming IKE messages even if a crypto map is not configured. Administrators who do not have a crypto map configured should also check that IKEv1 or IKEv2 is disabled on the affected system.

To verify that IKEv1 is enabled, use the following commands and verify that the command returns output:

- **show running-config crypto ikev1 | include enable** command for Cisco ASA Software releases 8.4 and later
- **show running-config crypto isakmp | include enable** command for Cisco ASA Software releases between 7.2.1 and 8.4
- **show running-config | include isakmp enable** command for Cisco ASA Software releases prior to 7.2.1

To verify that IKEv2 is enabled, use the **show running-config crypto ikev2 | include enable** and verify that it returns output.

Cisco ASA Software Configured as Easy VPN Hardware Client

Cisco ASA Software is affected by this vulnerability if the system is configured as an Easy VPN hardware client.

To verify that the system is configured as Easy VPN hardware client, use the **show running-config vpnclient | include enable** and verify that it returns output. The following example shows Cisco ASA configured as an Easy VPN hardware client:

```
ciscoasa# show running-config vpnclient | include enable
 vpnclient enable
```

Note: To exploit this vulnerability on Cisco ASA Software configured as an Easy VPN hardware client, an attacker must force the Cisco ASA to connect to a malicious VPN server.

Products Confirmed Not Vulnerable

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

Indicator of Compromise

Workarounds

There are no workarounds that address this vulnerability.

Fixed Software

Cisco has released free software updates that address the vulnerability described in this advisory. Customers may only install and expect support for software versions and feature sets for which they have purchased a license. By installing, downloading, accessing, or otherwise using such software upgrades, customers agree to follow the terms of the Cisco software license:
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html

Additionally, customers may only download software for which they have a valid license, procured from Cisco directly, or through a Cisco authorized reseller or partner. In most cases this will be a maintenance upgrade to software that was previously purchased. Free security software updates do not entitle customers to a new software license, additional software feature sets, or major revision upgrades.

When considering software upgrades, customers are advised to consult the Cisco Security Advisories and Responses archive at http://www.cisco.com/go/psirt and review subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should ensure that the devices to upgrade 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.

Customers Without Service Contracts

Customers who purchase directly from Cisco but do not hold a Cisco service contract and customers who make purchases through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should obtain upgrades by

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

ST 36903

ST 37674

IPS Cisco ASA Software IKEv1 and IKEv2 Buffer Overflow

Subscribe to Cisco Security Notifications

Subscribe

contacting the Cisco Technical Assistance Center (TAC):
http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

Customers should have the product serial number available and be prepared to provide the URL of this advisory as evidence of entitlement to a free upgrade.

Fixed Releases

In the following table, the left column lists major releases of Cisco ASA Software. The right column indicates whether a major release is affected by the vulnerability described in this advisory and the first release that includes the fix for this vulnerability.

Cisco ASA Major Release	First Fixed Release
7.2[1]	Affected; migrate to 9.1(6.11) or later
8.0[1]	Affected; migrate to 9.1(6.11) or later
8.1[1]	Affected; migrate to 9.1(6.11) or later
8.2[1]	8.2(5.59)[2]
8.3[1]	Affected; migrate to 9.1(6.11) or later
8.4	8.4(7.30) or later
8.5[1]	Not affected
8.6[1]	Affected; migrate to 9.1(6.11) or later
8.7	8.7(1.18) or later
9.0	9.0(4.38) or later
9.1	9.1(6.11) or later
9.2	9.2(4.5) or later
9.3	9.3(3.7) or later
9.4	9.4(2.4) or later
9.5	9.5(2.2) or later

[1] Cisco ASA Software releases 7.2, 8.0, 8.1, 8.2, 8.3, 8.5, and 8.6 have reached End of Software Maintenance. Customers should migrate to a supported release.
[2] Cisco ASA Software release 8.2 reached End of Software Maintenance on October 21, 2015. To protect our customers still using the End of Support train 8.2 software, the Cisco ASA product team has made available an off-cycle release to address this issue. As Cisco has no plans for additional off-cycle updates to train 8.2, we recommend customers work with their relevant support organization to migrate to supported software.

Software Download

Cisco ASA Software can be downloaded from the Software Center on Cisco.com by visiting http://www.cisco.com/cisco/software/navigator.html.

For Cisco ASA 5500 Series Adaptive Security Appliances and Cisco ASA 5500-X Series Next-Generation Firewall, navigate to the following path. To find interim versions, click **All Releases > Interim** on the left side of the download page.

> **Products > Security > Firewalls > Adaptive Security Appliances (ASA) > ASA 5500-X Series Firewalls > < your Cisco ASA model> > Software on Chassis > Adaptive Security Appliance (ASA) Software**

For the Cisco ASA Services Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers, navigate to the following path. To find interim versions, click **All Releases > Interim** on the left side of the download page.

> **Products > Cisco Interfaces and Modules > Services Modules > Catalyst 6500 Series / 7600 Series ASA Services Module > Adaptive Security Appliance (ASA) Software**

For the Cisco ASA 1000V Cloud Firewall, navigate to the following path:

> **Products > Security > Firewalls > Adaptive Security Appliances (ASA) > ASA 1000V Cloud Firewall**

For the Cisco Adaptive Security Virtual Appliance (ASAv), navigate to the following path:

> **Products > Security > Firewalls > Adaptive Security Appliances (ASA) > Adaptive Security Virtual Appliance (ASAv) > Adaptive Security Appliance (ASA) Software**

For the Cisco Firepower 9300 ASA Module, navigate to the following path:

> **Products > Security > Firewalls > Next-Generation Firewalls (NGFW) > Firepower 9000 Series > Firepower 9300 Security Appliance >Adaptive Security Appliance (ASA) Software**

For the Cisco ISA 3000 Industrial Security Appliance, navigate to the following path:

> **Products > Security > Firewalls > 3000 Series Industrial Security Appliances (ISA) > <your Cisco ISA 3000 model> > Adaptive Security Appliance (ASA) Software**

Exploitation and Public Announcements

The Cisco Product Security Incident Response Team (PSIRT) is not aware of any malicious use of the vulnerability that is described in this advisory.

Exodus Intelligence has provided a public blog post which is available at the following link:
https://blog.exodusintel.com/2016/02/10/firewall-hacking/

Source

This vulnerability was reported to Cisco by David Barksdale, Jordan Gruskovnjak, and Alex Wheeler of Exodus Intelligence.

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160210-asa-ike

---

Revision History

Version	Description	Section	Status	Date
1.2	Updated information in Vulnerable Products and Fixed Software section. Added additional signatures to Indicators of Compromise.	Vulnerable Products, Indicators of Compromise, Fixed Software	Final	2016-February-16
1.1	Updated Indicators of Compromise and Exploitation and Public Announcements with additional information	Indicators of Compromise, Exploitation and Public Announcements	Final	2016-February-11
1.0	Initial public release	-	Final	2016-February-10

Legal Disclaimer

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

A standalone copy or paraphrase of the text of this document that omits the distribution URL is an uncontrolled copy and may lack important information or contain factual errors. The information in this document is intended for end users of Cisco products.

Information For

Small Business
Midsize Business
Service Provider
Executives

Industries

Marketplace

Contacts

Contact Cisco
Find a Reseller

News & Alerts

Newsroom
Blogs
Field Notices
Security Advisories

Technology Trends

Cloud
Internet of Things (IoT)
Mobility
Software Defined Networking (SDN)

Support

Downloads
Documentation

Communities

DevNet
Learning Network
Support Community

Video Portal

About Cisco

Investor Relations
Corporate Social Responsibility
Environmental Sustainability
Tomorrow Starts Here
Our People

Careers

Search Jobs
Life at Cisco

Programs

Cisco Designated VIP Program
Cisco Powered
Financing Options

Contacts | Feedback | Help | Site Map | Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks