Worldwide | Log In | Account | Register

Products & Services Support How to Buy Training & Events Partners

Cisco Security Advisory

Cisco IOS and Cisco IOS XE Software OpenSSH TCP Denial of Service Vulnerability

Medium

Advisory ID:	cisco-sa-20160620-isr
Last Updated:	2016 August 18 19:47 GMT
Published:	2016 June 20 20:45 GMT
Version1.1:	Final
CVSS Score:	Base - 5.0
Workarounds:	No workarounds available
Cisco Bug IDs:	CSCuu13476

CVE-2015-6289
CWE-399

Download CVRF

Download PDF

Email

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.

Subscribe to Cisco Security Notifications

Subscribe

Summary

A vulnerability in the handling of Secure Shell (SSH) TCP packets in the Cisco IOS and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a partial denial of service (DoS) condition due to low memory on the device.

The vulnerability is due to the handling of out-of-order, or otherwise invalid, TCP packets on an SSH connection to the device. An attacker could exploit this vulnerability by connecting via SSH to the device and then crafting TCP packets which are out of order or have invalid flags. An exploit could allow the attacker to cause the device to report low-memory warnings which could in turn cause a partial DoS condition.

Cisco will release software updates that address this vulnerability. Please refer to the Cisco Bug Search Tool link as described in the "Fixed Software" section for information about software availability. Workarounds that address this vulnerability are not available.

This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160620-isr

Affected Products

Vulnerable Products

Cisco IOS and Cisco IOS XE Software are vulnerable.

Products Confirmed Not Vulnerable

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

Workarounds

Workarounds that mitigate this vulnerability are not available.

Fixed Software

Cisco provides information about fixed software in Cisco bugs, which are accessible through the Cisco Bug Search Tool.

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 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.

Exploitation and Public Announcements

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.

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160620-isr

Revision History

Version	Description	Section	Status	Date
1.1	This vulnerability affects Cisco IOS and IOS XE Software. Cisco will release software updates for this vulnerability.	Title, Vulnerable Products, and Summary	Final	2016-August-18
1.0	Initial public release.	-	Final	2016-June-20

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