Cisco Security Advisory

Cisco Adaptive Security Device Manager Remote Code Execution Vulnerability

Medium

Advisory ID:
cisco-sa-asdm-rce-gqjShXW

First Published:
2021 July 7 16:00 GMT

Last Updated:
2021 August 5 15:49 GMT

Version 1.2: Final

Workarounds: No workarounds available

Cisco Bug IDs:
CSCvw79912

CVE-2021-1585

CWE-94

CVSS Score:
Base 7.5

Download CVRF Email

Summary

A vulnerability in the Cisco Adaptive Security Device Manager (ASDM) Launcher could allow an unauthenticated, remote attacker to execute arbitrary code on a user's operating system.

This vulnerability is due to a lack of proper signature verification for specific code exchanged between the ASDM and the Launcher. An attacker could exploit this vulnerability by leveraging a man-in-the-middle position on the network to intercept the traffic between the Launcher and the ASDM and then inject arbitrary code. A successful exploit could allow the attacker to execute arbitrary code on the user's operating system with the level of privileges assigned to the ASDM Launcher. A successful exploit may require the attacker to perform a social engineering attack to persuade the user to initiate communication from the Launcher to the ASDM.

Cisco has not released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

This advisory is available at the following link:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asdm-rce-gqjShXW

Affected Products

Vulnerable Products

At the time of publication, this vulnerability affected Cisco ASDM releases 7.16(1.150) and earlier.

See the Details section in the bug ID(s) at the top of this advisory for the most complete and current information.

Products Confirmed Not Vulnerable

Only products listed in the Vulnerable Products section of this advisory are known to be affected by this vulnerability.

Details

An attacker could also leverage a man-in-the-middle position to persuade the user to retrieve an arbitrary file as part of the communication between the Launcher and the ASDM. This secondary drive-by download vulnerability has a CVSS score of 3.1 (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N) and is addressed by the bug ID at the top of this advisory.

Workarounds

There are no workarounds that address this vulnerability.

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 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

At the time of publication, Cisco planned to fix this vulnerability in Cisco ASDM. See the Details section in the bug ID(s) at the top of this advisory for the most complete and current information.

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.

Source

Cisco would like to thank security researcher Malcolm Lashley for reporting these vulnerabilities.

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asdm-rce-gqjShXW

Revision History

Version	Description	Section	Status	Date
1.2	Added clarifications about future fixes.	Summary, Fixed Software	Final	2021-AUG-05
1.1	Updated the vulnerable releases.	Vulnerable Products	Final	2021-JUL-13

Show Complete History...

Legal Disclaimer

Cisco Security Vulnerability Policy

Subscribe to Cisco Security Notifications

Your Rating:

Average Rating:

5 star	0
4 star	1
3 star	1
2 star	1
1 star	1

Leave additional feedback