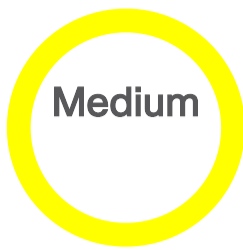


 Unleash the Power of TAC's Virtual Assistance ×
Activate Cisco In Product Support ▶

Cisco Secure Web Appliance Authentication Bypass Vulnerability

**Advisory ID:**

cisco-sa-wsa-auth-bypass-6YZkTQhd

First Published:

2026 April 15 16:00 GMT


Last Updated:

2026 April 16 13:14 GMT

Version 1.1: [Final](#)**Workarounds:** No workarounds available**Cisco Bug IDs:**[CSCwr20696](#)

CVE-2026-20152

CWE-305

CVSS Score:[Base 5.3](#) [Download CSAF](#)[Email](#)

^ Summary

A vulnerability in the authentication service feature of Cisco AsyncOS Software for Cisco Secure Web Appliance could allow an unauthenticated, remote attacker to bypass authentication policy requirements.

This vulnerability is due to improper validation of user-supplied authentication input in HTTP requests. An attacker could exploit this vulnerability by sending HTTP requests that contain specific authentication requests to an affected device. A successful exploit could allow the attacker to bypass policy enforcement on the device. There is no direct impact to the Cisco Secure Web Appliance. However, as a result of exploiting this vulnerability, an attacker could send HTTP requests that should be restricted through the device.

Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

This advisory is available at the following link:

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-auth-bypass-6YZkTQhd>

^ Affected Products

Vulnerable Products

At the time of publication, this vulnerability affected Cisco Secure Web Appliance, both virtual and hardware versions.

For information about which Cisco software releases were vulnerable at the time of publication, see the [Fixed Software](#) section of this advisory. 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.

Cisco has confirmed that this vulnerability does not affect the following Cisco products:

- Secure Email Gateway, both virtual and hardware appliances
- Secure Email and Web Manager, both virtual and hardware appliances

^ Workarounds

There are no workarounds that address this vulnerability.

^ Fixed Software

Cisco considers any workarounds and mitigations (if applicable) to be temporary solutions until an upgrade to a fixed software release is available. To fully remediate this vulnerability and avoid future exposure as described in this advisory, Cisco strongly recommends that customers upgrade to the fixed software indicated in this advisory.

Fixed Releases

At the time of publication, the release information in the following table was accurate. See the Details section in the bug ID(s) at the top of this advisory for the most complete and current information.

The left column lists Cisco software releases, and the right column indicates whether a release was affected by the vulnerability that is described in this advisory and which release included the fix for this vulnerability.

Cisco AsyncOS Software for Cisco Secure Web Appliance Release	First Fixed Release
Earlier than 15.2	Migrate to a fixed release.
15.2	15.2.5-013
15.5	Migrate to a fixed release.
16.0	Not affected.

The Cisco Product Security Incident Response Team (PSIRT) validates only the affected and fixed release information that is documented in this advisory.

^ Exploitation and Public Announcements

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

^ Source

This vulnerability was found during the resolution of a Cisco Technical Assistance Center (TAC) support case.

^ URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-auth-bypass-6YZkTQhd>

^ Revision History

Version	Description	Section	Status	Date
1.1	Updated fixed releases with information for Release 15.5.	Fixed Software	Final	2026-APR-16
1.0	Initial public release.	-	Final	2026-APR-15

^ Legal Disclaimer

SOFTWARE DOWNLOADS AND TECHNICAL SUPPORT


The [Cisco Support and Downloads](#) page on Cisco.com provides information about licensing and downloads. This page can also display customer device support coverage for customers who use the My Devices tool. Please note that customers may download only software that was procured from Cisco directly or through a Cisco authorized reseller or partner and for which the license is still valid.

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 contacting the [Cisco Technical Assistance Center \(TAC\)](#). 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.

When [considering software upgrades](#), customers are advised to regularly consult [the advisories](#) for the relevant Cisco products 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.

LEGAL DISCLAIMER DETAILS

CISCO DOES NOT MAKE ANY EXPRESS OR IMPLIED GUARANTEES OR WARRANTIES OF ANY KIND, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, CISCO DOES NOT GUARANTEE THE ACCURACY OR COMPLETENESS OF THIS INFORMATION. THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS. 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.

 Unleash the Power of TAC's Virtual Assistance x
 Activate Cisco In Product Support >

Copies or summaries of the information contained in this Security Advisory may lack important information or contain factual errors. Customers are advised to visit the [Cisco Security Advisories](#) page for the most recent version of this Security Advisory. The Cisco Product Security Incident Response Team (PSIRT) assesses only the affected and fixed release information that is documented in this advisory. See the [Cisco Security Vulnerability Policy](#) for more information.

▶ [Cisco Security Vulnerability Policy](#)

▶ [Subscribe to Cisco Security Notifications](#)

▶ [Related to This Advisory](#)

 **Unleash the Power of TAC's Virtual Assistance** ×
Cisco [Activate Cisco In Product Support](#) ▶