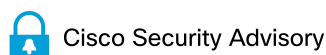
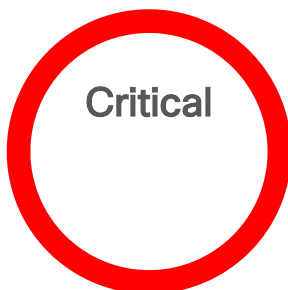


[Home](#) / [Cisco Security](#) / [Security Advisories](#)

# Cisco Smart Software Manager On-Prem Arbitrary Command Execution Vulnerability

**Advisory ID:**

cisco-sa-ssm-cli-execution-cHUcWuNr

**First Published:**

2026 April 1 16:00 GMT

**Version 1.0:**

Final

**Workarounds:**

No workarounds available

**Cisco Bug IDs:**[CSCws84279](#)

CVE-2026-20160

CWE-668

**CVSS Score:**Base 9.8 [Download CSAF](#)[Email](#)

## Summary

A vulnerability in Cisco Smart Software Manager On-Prem (SSM On-Prem) could allow an unauthenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected SSM On-Prem host.

This vulnerability is due to the unintentional exposure of an internal service. An attacker could exploit this vulnerability by sending a crafted request to the API of the exposed service. A successful exploit could allow the attacker to execute commands on the underlying operating system with *root*-level privileges.

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-ssm-cli-execution-cHUcWuNr>

## Affected Products

### Vulnerable Products

This vulnerability affects Cisco SSM On-Prem, regardless of the software configuration.

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

## 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:

- Smart Licensing Utility
- Smart Software Manager satellite

## ^ 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

In the following table, the left column lists Cisco software releases. The right column indicates whether a release is affected by the vulnerability that is described in this advisory and the first release that includes the fix for this vulnerability. Customers are advised to upgrade to an appropriate [fixed software release](#) as indicated in this section.

Cisco SSM On-Prem Release	First Fixed Release
Earlier than 9-202502	Not vulnerable
9-202502 to 9-202510	9-202601

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-ssm-cli-execution-cHUcWuNr>

## ^ Revision History

Version	Description	Section	Status	Date
1.0	Initial public release.	-	Final	2026-APR-01

## ^ 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.

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](#)

---