Hive Pro

Threat Level

Amber

Hiveforce Labs

# THREAT ADVISORY

## VULNERABILITY REPORT

# Cisco SSM On-Prem Flaw Lets Hackers Hijack User Passwords

| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| August 9, 2024 | A1 | TA2024306 |

# Summary

**First Seen:** July 2024
**Affected Products:** Cisco Smart Software Manager On-Prem (SSM On-Prem)
**Impact:** Cisco has addressed a critical vulnerability, CVE-2024-20419, which could allow attackers to change any user's password, including administrators, on vulnerable SSM On-Prem servers. Cisco has also issued a warning that exploit code for this maximum-severity flaw is now publicly available, increasing the urgency for affected organizations to apply the patch.

## CVE

| CVE | NAME | AFFECTED PRODUCTS | ZERO-DAY | CISA | PATCH |
|---|---|---|---|---|---|
| CVE-2024-20419 | Cisco Smart Software Manager On-Prem Password Change Vulnerability | Cisco Smart Software Manager On-Prem (SSM On-Prem) | ✗ | ✗ | ✓ |

# Vulnerability Details

**#1** A critical vulnerability, identified as CVE-2024-20419, has been discovered in Cisco's Smart Software Manager On-Prem (SSM On-Prem), which permits unauthenticated remote attackers to alter user passwords, including those of administrative users. This flaw presents a significant security threat, underscoring the necessity for immediate action to prevent potential exploitation.

**#2** The Cisco Smart Software Manager On-Prem (SSM On-Prem) license server is a vital component of Cisco's Smart Licensing ecosystem. It operates in tandem with the cloud-based Cisco Smart Software Manager to facilitate the intelligent management of customer product licenses, providing near-real-time visibility and reporting on license acquisition and usage.

**#3** The root cause of the vulnerability is the lack of proper validation of the old password before setting a new one. This weakness allows remote attackers to send malicious HTTP requests, potentially gaining unauthorized access to the web UI or API with the compromised user's privileges. No workarounds are currently available for affected systems, making it imperative for administrators to upgrade to a fixed release to secure their vulnerable SSM On-Prem servers. The existence of proof-of-concept exploit code further elevates the urgency of applying the necessary patches.

## Vulnerability

| CVE ID | AFFECTED PRODUCTS | AFFECTED CPE | CWE ID |
|---|---|---|---|
| CVE-2024-20419 | Cisco SSM On-Prem: Version 8-202206 and earlier | cpe:2.3:a:cisco:smart_software_manager_on-prem:8-202206:*:*:*:*:*:*:* | CWE-620 |

# Recommendations

**Update:** To mitigate the risk associated with CVE-2024-20419, users are strongly urged to upgrade Cisco SSM On-Prem to version 8-202212. This update addresses the vulnerability and enhances the overall security.

**Monitoring Password Change Activities:** Continuously monitor system and application logs for password change events. Set up alerts for anomalies, such as multiple password changes within a short period or changes outside of normal working hours. Conduct periodic audits of password change logs to detect any irregularities or patterns that could indicate malicious activity.

**Limit Exposure:** Restrict access to critical systems and endpoints to minimize potential attack vectors. Implement strict network access controls to ensure that only authorized users and systems can interact with sensitive components.

## Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| TA0042<br>Resource Development | TA0001<br>Initial Access | TA0004<br>Privilege Escalation | TA0006<br>Credential Access |
| T1190<br>Exploit Public-Facing Application | T1068<br>Exploitation for Privilege Escalation | T1588<br>Obtain Capabilities | T1588.006<br>Vulnerabilities |

## Patch Details

Users are strongly urged to upgrade their Cisco SSM On-Prem to version 8-202212. This update addresses the CVE-2024-20419 and enhances the overall security.

Link:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cssm-auth-sLw3uhUy#fs

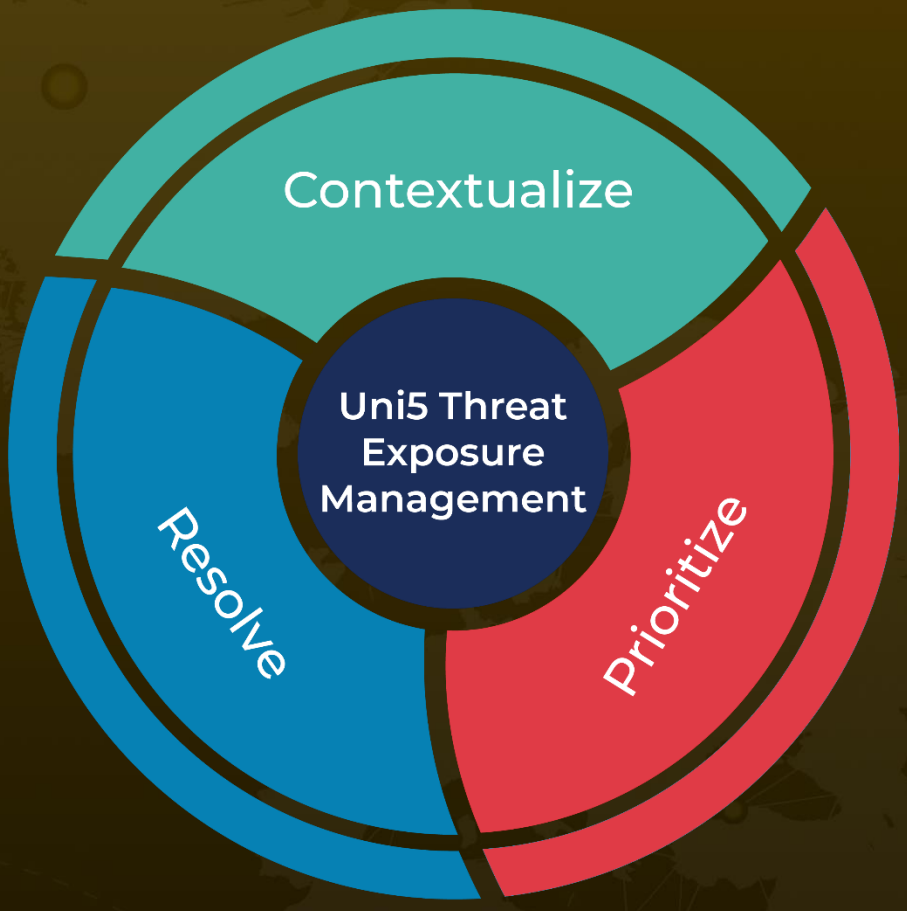
## References

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cssm-auth-sLw3uhUy

# What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.




REPORT GENERATED ON

**August 9, 2024 • 6:30 AM**



More at www.hivepro.com