National Cyber Security Centre

2407180179-NCSC

**Department of the Environment, Climate & Communications**

# NCSC Alert

## Critical Vulnerability exists in Cisco Smart Software Manager On-Prem (CVE-2024-20419, CVSSv3: 10.0)

Thursday 18th July, 2024

**STATUS:** TLP-CLEAR

*Recipients can spread this to the world, there is no limit on disclosure. Sources may use* TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction.*
For more information on the Traffic Light Protocol, see https://www.first.org/tlp/.
Please treat this document in accordance with the TLP assigned.

## Description

**Published:** 2024-07-17T17:15:00
**Vendor:** Cisco
**Product:** Cisco Smart Software Manager On-Prem
**CVE ID:** CVE-2024-20419
**CVSS3.0 Score**[1]**:** 10.0
**EPSS**[2]**:** 0.093060000
(For up to date EPSS score, click here: https://api.first.org/data/v1/epss?cve=CVE-2024-20419
**Summary:** A vulnerability in the authentication system of Cisco Smart Software Manager On-Prem (SSM On-Prem) could allow an unauthenticated, remote attacker to change the password of any user, including administrative users.

This vulnerability is due to improper implementation of the password-change process. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow an attacker to access the web UI or API with the privileges of the compromised user.

## Products Affected

- Cisco Cisco Smart Software Manager On-Prem

## Impact

- **Common Weakness Enumeration (CWE)**[3]**:** CWE-620 - Unverified Password Change
- **Present in CISA Known Exploited Vulnerability(KEV)**[4] **catalog:** NO
- **Used by Ransomware Operators:** Not Known

## Recommendations

The NCSC strongly advises affected organisations to review the latest release notes and install the relevant updates from Cisco.

Additional recommendations and mitigations for CVE-2024-20419 can be found in the respective link below:

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

[1] https://www.first.org/cvss/v3.0/specification-document
[2] https://www.first.org/epss/articles/prob_percentile_bins
[3] https://cwe.mitre.org/
[4] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

**DISCLAIMER:** This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
Tom Johnson House,
Beggars Bush,
Dublin, D04 A068,
Ireland
**Tel:** +353 (0)1 6782333
**Mail:** certreport@ncsc.gov.ie
**Web:** ncsc.gov.ie
**Twitter:** ncsc_gov_ie
**LinkedIn:** ncsc-ie


**An Lárionad Náisiúnta Cibearshlándála**
National Cyber Security Centre