Security Advisory 2024-070

Critical Vulnerabilities in Cisco Products

July 18, 2024 — v1.0

TLP:CLEAR

History:

- *18/07/2024 — v1.0 – Initial publication*

Summary

On July 17, 2024, Cisco issued several security advisories addressing critical and high severity vulnerabilities in its products. It is strongly recommended applying update on affected devices as soon as possible, prioritising internet facing and business critical devices.

Technical Details

The critical vulnerability **CVE-2024-20401**, with a CVSS score of 9.8, is an arbitrary file write flaw [1]. It affects the content scanning and message filtering features of Cisco Secure Email Gateway and is due to improper handling of email attachments when file analysis and content filters are enabled. A successful exploit could allow the attacker to replace any file on the underlying file system. The attacker could then perform any of the following actions: add users with root privileges, modify the device configuration, execute arbitrary code, or cause a permanent denial of service (DoS) condition on the affected device.

The critical vulnerability **CVE-2024-20419**, with a CVSS score of 10, lies 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 [2]. 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.

The list of all vulnerabilities could be found in the vendor's website.

Affected Products

The vulnerability **CVE-2024-20401** affects Cisco Secure Email Gateway if it is running a vulnerable release of Cisco AsyncOS (version prior to `15.5.1-055`) and both of the following conditions are met:

- Either the file analysis feature, which is part of Cisco Advanced Malware Protection (AMP), or the content filter feature is enabled and assigned to an incoming mail policy
- The Content Scanner Tools version is earlier than 23.3.0.4823

The vulnerability **CVE-2024-20419** affects Cisco SSM On-Prem and Cisco Smart Software Manager Satellite (SSM Satellite) version `8-202206` and earlier.

Note: Cisco SSM On-Prem and Cisco SSM Satellite are the same product. For releases earlier than Release 7.0, this product was called Cisco SSM Satellite. As of Release 7.0, this product is called Cisco SSM On-Prem.

Recommendations

CERT-EU strongly recommends updating affected products as soon as possible to mitigate these vulnerabilities, prioritising Internet facing and business critical devices.

References

[1] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-afw-bGG2UsjH

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