CYBER ADVISORY

TLP:CLEAR
17 July 2024

Multiple Cisco Vulnerabilities

Cisco | Static Key | Email Gateway | Critical Vulnerability

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of multiple high and critical vulnerabilities affecting Cisco products.[1] Exploitation of the most critical of the vulnerabilities could provide an attacker the ability to remotely overwrite arbitrary files on an underlying operating system, or remotely change the password of any user, to include administrative users.[2,3]

Affected Cisco Product(s)	Issue	CVE Identifier(s)
Content Scanner Tools version earlier than v23.3.0.4823	Allows an unauthenticated, remote attacker to overwrite arbitrary files on the underlying operating system.	CVE-2024-20401
Cisco SSM On-Prem and Cisco SSM Satellite. (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.)	Allows an unauthenticated, remote attacker to change the password of any user, including administrative users.	CVE-2024-20419
Cisco AsyncOS for Secure Web Appliance, both virtual and hardware appliances v14.5 and earlier	Allows an authenticated, local attacker to execute arbitrary commands and elevate privileges to *root*.	CVE-2024-20435
Cisco ISE in the default configuration v3.0 and earlier	Allows an authenticated, remote attacker to upload arbitrary files to an affected device	CVE-2024-20296
Cisco iNode Software v3.1.2 and earlier and Cisco iNode Manager Software v23.1 and earlier	Allows an unauthenticated, remote attacker to hijack the TLS connection between Cisco iNode Manager and associated intelligent nodes and send arbitrary traffic to an affected device	CVE-2024-20323

Table 1: Vulnerable Cisco Products (Critical and High)

In addition to the above referenced vulnerabilities, the following table provides information on medium vulnerabilities affecting Cisco Products:

Affected Cisco Product(s)	Issue	CVE Identifier(s)
• RV340 Dual WAN Gigabit VPN Routers • RV340W Dual WAN Gigabit Wireless-AC VPN Routers • RV345 Dual WAN Gigabit VPN Routers • RV345P Dual WAN Gigabit PoE VPN Routers	Allows an authenticated, remote attacker to execute arbitrary code on an affected device	CVE-2024-20416
Cisco Expressway Series Release earlier than v15	Allows an unauthenticated, remote attacker to redirect a user to a malicious web page	CVE-2024-20400
Cisco AsyncOS for Secure Email Gateway v14.2 and earlier, and v15.0	Allows an authenticated, remote attacker to execute arbitrary system commands on an affected device	CVE-2024-20429

Table 2: Vulnerable Cisco Products (Medium)

The Cal-CSIC recommends immediately upgrading all affected Cisco Products to the current patched versions.

For further information on upgrading affected Cisco products, please refer to Security Vulnerability Policy (cisco.com)

Organization, Source, Reference, and Dissemination Information

Organization Description	California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of

	cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.
Customer Feedback	If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1. To help us identify ways to better assist you, please submit feedback calcsic@caloes.ca.gov.
Source Summary Statement	This report was compiled from a variety of sources, predominately open-source reporting.
Handling Caveats	**Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.
Information Needs	*HSEC 1.1; HSEC 1.2; HSEC 1.5; HSEC 1.8; HSEC 1.10; STAC KIQ 1.1; KIQ 1.2; KIQ 1.3; KIQ 1.4; KIQ 1.5*

---

[1] Cisco Security; "Cisco Security Advisories;" https://sec.cloudapps.cisco.com/security/center/publicationListing.x; accessed 17 July 2024

[2] CVE.org; "CVE-2024-20401;" https://www.cve.org/CVERecord?id=CVE-2024-20401; accessed 17 July 2024

[3] Bleeping Computer: "Cisco SSM On-Prem but lets hackers change any user's password;" https://www.bleepingcomputer.com/news/security/cisco-ssm-on-prem-bug-lets-hackers-change-any-users-password/; accessed 17 July 2024