CYBER ADVISORY

TLP:CLEAR
25 April 2024

CISCO ASA and FTD Zero-Day Vulnerabilities

CVE-2024-20359 | CVE-2024-20353 | Active Exploitation | High Vulnerabilities

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of high zero-day vulnerabilities, under active exploitation, as part of an espionage campaign known as CVE-2024-20359 and CVE-2024-20353.[1] The vulnerabilities affect Cisco's Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) Software.[2] Exploitation of CVE-2024-20359 may allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability.[3] Exploitation of CVE-2024-20353 may allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.[4]

The Cal-CSIC recommends immediately applying Cisco ASA and/or FTD software updates.

For further information on applying Cisco software updates, please refer to Cisco Security Portal.

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] The Hacker News; "State-Sponsored Hackers Exploit Two Cisco Zero-Day Vulnerabilities for Espionage;" https://thehackernews.com/2024/04/state-sponsored-hackers-exploit-two.html; accessed 25 April 2024

[2] Bleeping Computer; "ArcaneDoor hackers exploit Cisco zero-days to breach govt networks;" https://www.bleepingcomputer.com/news/security/arcanedoor-hackers-exploit-cisco-zero-days-to-breach-govt-networks/; accessed 25 April 2024

[3] Cisco; "Cisco Adaptive Security Appliance and Firepower Threat Defense Software Persistent Local Code Execution Vulnerability;" https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h; accessed 25 April 2024

[4] Cisco; "Cisco Adaptive Security Appliance and Firepower Threat Defense Software Web Services Denial of Service Vulnerability;" https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2; accessed 25 April 2024