مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Exploited Vulnerabilities in Cisco ASA & FTD Products

Tracking #:432315787

Date:25-04-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in CISCO ASA & FTD that are being actively exploited by threat actors to gain unauthorized access.

TECHNICAL DETAILS:

Cisco has released security updates to address the exploitation of Cisco Adaptive Security Appliances (ASA) devices and Cisco Firepower Threat Defense (FTD) software. These vulnerabilities, CVE-2024-20353, CVE-2024-20359, and CVE-2024-20358, could allow a cyber threat actor to take control of an affected system.

Cisco has reported active exploitation of CVE-2024-20353 and CVE-2024-20359. These vulnerabilities allow unauthenticated remote attackers to exploit them and potentially gain persistence on affected devices. This campaign, dubbed ArcaneDoor by Cisco, has been actively exploited by state-sponsored actors since at least November 2023.

Vulnerability Details:

CVE & Vulnerability	Severity	Cisco Advisory
CVE-2024-20359- Cisco Adaptive Security Appliance and Firepower Threat Defense Software Persistent Local Code Execution Vulnerability	High	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h#vp
CVE-2024-20353- Cisco Adaptive Security Appliance and Firepower Threat Defense Software Web Services Denial of Service Vulnerability	High	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2
CVE-2024-20358- Cisco Adaptive Security Appliance and Firepower Threat Defense Software Command Injection Vulnerability	Medium	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm

Affected Products:

- Cisco Adaptive Security Appliance (ASA) Software
- Cisco Firepower Threat Defense (FTD) Software

Fixed Versions:

Refer Cisco Advisory

RECOMMENDATIONS:

- Immediate patching: Patch all Cisco ASA and FTD devices with the latest software updates as soon as possible.
- Threat hunting and investigation: Organizations are advised to investigate their systems for indicators of compromise (IOCs) associated with this campaign.
- Review configurations: Scrutinize firewall configurations for unauthorized changes.
- Monitor logs: Closely monitor system logs for suspicious activity, including undocumented configuration changes, unexpected reboots, and anomalous credential use.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

1. https://nvd.nist.gov/vuln/detail/CVE-2024-20353
2. https://nvd.nist.gov/vuln/detail/CVE-2024-20359
3. https://nvd.nist.gov/vuln/detail/CVE-2024-20358