مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates-Multiple Vulnerabilities Cisco Products

Tracking #:432315684

Date:07-03-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Cisco recently released security advisories to address multiple vulnerabilities in its products.

TECHNICAL DETAILS:

On March 6, 2024, Cisco released security advisories addressing several vulnerabilities in its products, **including two high-severity vulnerabilities**. Successful exploitation of these vulnerabilities could allow attackers to escalate privileges, inject malicious code, bypass authentication, or leak sensitive information on affected systems.

Vulnerabilities Details:

CVE	Severity	Description
CVE-2024-20338	High	Cisco Secure Client for Linux with ISE Posture Module Privilege Escalation Vulnerability
CVE-2024-20337	High	Cisco Secure Client Carriage Return Line Feed Injection Vulnerability
CVE-2024-20335, CVE-2024-20336	Medium	Cisco Small Business 100, 300, and 500 Series Wireless Access Points Command Injection and Buffer Overflow Vulnerabilities
CVE-2024-20301	Medium	Cisco Duo Authentication for Windows Logon and RDP Authentication Bypass Vulnerability
CVE-2024-20292	Medium	Cisco Duo Authentication for Windows Logon and RDP Information Disclosure Vulnerability
CVE-2024-20346	Medium	Cisco AppDynamics Controller Cross-Site Scripting Vulnerability
CVE-2024-20345	Medium	Cisco AppDynamics Controller Path Traversal Vulnerability

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by Cisco.

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:

https://sec.cloudapps.cisco.com/security/center/publicationListing.x