مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates- Multiple Vulnerabilities Cisco Products

Tracking #:432315701

Date:14-03-2024

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

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

TECHNICAL DETAILS:

Cisco has released security updates to address multiple vulnerabilities in its products. These vulnerabilities could potentially be exploited by malicious actors to gain unauthorized access, cause denial-of-service (DoS) conditions, or escalate privileges on affected systems.

Vulnerabilities Details:

CVE	Severity	Description
CVE-2023-20214	Critical	Cisco SD-WAN vManage Unauthenticated REST API Access Vulnerability
CVE-2024-20318	High	Cisco IOS XR Software Layer 2 Services Denial of Service Vulnerability
CVE-2024-20320	High	Cisco IOS XR Software SSH Privilege Escalation Vulnerability
CVE-2024-20327	High	Cisco IOS XR Software for ASR 9000 Series Aggregation Services Routers PPPoE Denial of Service Vulnerability
CVE-2024-20337	High	Cisco Secure Client Carriage Return Line Feed Injection Vulnerability
CVE-2024-20319	Medium	Cisco IOS XR Software SNMP Management Plane Protection ACL Bypass Vulnerability
CVE-2024-20262	Medium	Cisco IOS XR Software Authenticated CLI Secure Copy Protocol and SFTP Denial of Service Vulnerability
CVE-2024-20266	Medium	Cisco IOS XR Software DHCP Version 4 Server Denial of Service Vulnerability
CVE-2024-20315 CVE-2024-20322	Medium	Cisco IOS XR Software MPLS and Pseudowire Interfaces Access Control List Bypass Vulnerabilities
CVE-2023-20236	Medium	Cisco IOS XR Software iPXE Boot Signature Bypass 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