مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Cisco Security Updates

Tracking #:432316335

Date:26-09-2024

EXECUTIVE SUMMARY:

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

TECHNICAL DETAILS:

Cisco has released a security advisory addressing multiple vulnerabilities in its products. These vulnerabilities, if exploited, could lead to severe consequences such as unauthorized access, denial of service, and privilege escalation.

Vulnerabilities Details:

Description	Severity	CVE
Cisco IOS XE Software Web UI Cross-Site Request Forgery Vulnerability	High	CVE-2024-20437
Cisco Catalyst SD-WAN Routers Denial of Service Vulnerability	High	CVE-2024-20455
Cisco IOS and IOS XE Software Resource Reservation Protocol Denial of Service Vulnerability	High	CVE-2024-20433
Cisco IOS XE Software Protocol Independent Multicast Denial of Service Vulnerability	High	CVE-2024-20464
Cisco IOS XE Software SD-Access Fabric Edge Node Denial of Service Vulnerability	High	CVE-2024-20480
Cisco IOS XE Software HTTP Server Telephony Services Denial of Service Vulnerability	High	CVE-2024-20436
Cisco Catalyst Center Static SSH Host Key Vulnerability	High	CVE-2024-20350
Cisco IOS XE Software IPv4 Fragmentation Reassembly Denial of Service Vulnerability	High	CVE-2024-20467
Multiple Cisco Products Web-Based Management Interface Privilege Escalation Vulnerability	High	CVE-2024-20381
Cisco Catalyst 9000 Series Switches Denial of Service Vulnerability	Medium	CVE-2024-20434
Cisco Unified Threat Defense Snort Intrusion Prevention System Engine for Cisco IOS XE Software Security Policy Bypass and Denial of Service Vulnerability	Medium	CVE-2024-20508
Cisco Catalyst SD-WAN Manager Cross-Site Scripting Vulnerability	Medium	CVE-2024-20475
Cisco SD-WAN vEdge Software UDP Packet Validation Denial of Service Vulnerability	Medium	CVE-2024-20496
Cisco IOS Software on Cisco Industrial Ethernet Series Switches Access Control List Bypass Vulnerability	Medium	CVE-2024-20465
Cisco IOS and IOS XE Software Web UI Cross-Site Request Forgery Vulnerability	Medium	CVE-2024-20414
Cisco IOS XE Software for Wireless Controllers CWA Pre-Authentication ACL Bypass Vulnerability	Medium	CVE-2024-20510

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