



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Cisco Security Updates

Tracking #:432315734

Date:28-03-2024

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 INTELLIGENCE 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 advisories to address multiple vulnerabilities in its products.

TECHNICAL DETAILS:

On March 27, 2024, Cisco released security advisories addressing several vulnerabilities in multiple Cisco products. If exploited, these vulnerabilities could allow remote, unauthenticated attackers to gain unauthorized network access or launch denial-of-service (DoS) attacks on affected devices.

Vulnerabilities Details:

CVE	Impact	Description
CVE-2024-20271	High	Cisco Access Point Software Denial of Service Vulnerability
CVE-2024-20265	High	Cisco Access Point Software Secure Boot Bypass Vulnerability
CVE-2024-20259	High	Cisco IOS XE Software DHCP Snooping with Endpoint Analytics Denial of Service Vulnerability
CVE-2024-20307 CVE-2024-20308	High	Cisco IOS and IOS XE Software Internet Key Exchange Version 1 Fragmentation Denial of Service Vulnerabilities
CVE-2024-20276	High	Cisco IOS Software for Catalyst 6000 Series Switches Denial of Service Vulnerability
CVE-2024-20314	High	Cisco IOS XE Software SD-Access Fabric Edge Node Denial of Service Vulnerability
CVE-2024-20313	High	Cisco IOS XE Software OSPFv2 Denial of Service Vulnerability
CVE-2024-20311	High	Cisco IOS and IOS XE Software Locator ID Separation Protocol Denial of Service Vulnerability
CVE-2024-20303	High	Cisco IOS XE Software for Wireless LAN Controllers Multicast DNS Denial of Service Vulnerability
CVE-2024-20312	High	Cisco IOS and IOS XE Software Intermediate System-to-Intermediate System Denial of Service Vulnerability

RECOMMENDATIONS:

The UAE Cyber Security Council recommends apply these updates as soon as possible to mitigate the risks associated with these vulnerabilities.

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>