مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates- Cisco

Tracking #:432316481

Date:07-11-2024

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

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Cisco has published security updates addressing multiple vulnerabilities in its products.

TECHNICAL DETAILS:

Vulnerability Details:

1. **CVE-2024-20418**-Cisco Unified Industrial Wireless Software for Ultra-Reliable Wireless Backhaul Access Point Command Injection Vulnerability
    - Severity: Critical (CVSS 10.0)
    - Description: A vulnerability exists in the web-based management interface of Cisco Unified Industrial Wireless Software for Cisco Ultra-Reliable Wireless Backhaul (URWB) Access Points. This flaw allows unauthenticated remote attackers to perform command injection attacks, potentially executing arbitrary commands with root privileges on the affected device's operating system.
    - Affected Products:
        - Cisco Catalyst IW9165D Heavy Duty Access Points
        - Cisco Catalyst IW9165E Rugged Access Points and Wireless Clients
        - Cisco Catalyst IW9167E Heavy Duty Access Points
    - Fixed Version: Cisco Unified Industrial Wireless Software Release-17.15.1

2. **CVE-2024-20536-**Cisco Nexus Dashboard Fabric Controller SQL Injection Vulnerability
    - Severity: High (CVSS 8.8)
    - Description: A vulnerability in Cisco Nexus Dashboard Fabric Controller (NDFC) allows authenticated remote attackers with read-only privileges to execute arbitrary SQL commands on the internal database through a vulnerable REST API endpoint or web-based management interface.
    - Affected Products: Cisco NDFC releases 12.1.2 and 12.1.3.
    - Fixed Version: Cisco NDFC 12.2

3. **CVE-2024-20484-** Cisco Enterprise Chat and Email Denial of Service Vulnerability
    - Severity: High (CVSS 7.5)
    - Description: A vulnerability exists in the External Agent Assignment Service (EAAS) feature of Cisco Enterprise Chat and Email (ECE) that could allow an unauthenticated, remote attacker to trigger a Denial of Service (DoS) condition on an affected device.
    - Affected Products:Cisco Enterprise Chat and Email (ECE) running the EAAS feature.
    - Fixed Versions: Cisco ECE Release- 12.5(1) ES9, 12.6(1) ES9 ET3

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

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/content/CiscoSecurityAdvisory/cisco-sa-backhaul-ap-cmdinj-R7E28Ecs
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndfc-sqli-CyPPAxrL
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ece-dos-Oqb9uFEv