Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No. 245 **02-4-2024**

Name: Cisco IOS Bugs Allow Unauthenticated, Remote DoS Attacks

Threat Classification: Denial-of-Service (DoS), Privilege Escalation, Command Injection

Affected Software / Area:

- Cisco IOS
- Cisco IOS XE
- Cisco Access Point Software

Summary:

Cisco has issued security updates for its IOS and IOS XE operating system software, as well as patches for its Access Point software. These updates address a total of 14 vulnerabilities, with 10 of them being denial-of-service (DoS) bugs that can lead to system crashes, unexpected reloads, and heap overflow. The most critical of these vulnerabilities allow unauthenticated, remote attackers to exploit the system. Additionally, other vulnerabilities include privilege escalation, command injection, and access control list bypass.

Severity	**High**
Attack Vector	Remote Code Execution

CVE's

CVE-2024-20265	**CVE-2024-20271**

Recommendations:

- Immediately apply the provided security updates for Cisco IOS, IOS XE, and Access Point Software to mitigate the identified vulnerabilities.
- Implement monitoring mechanisms to detect any unauthorized access attempts or suspicious activity targeting Cisco networking gear.
- Review and strengthen access controls to restrict access to critical network devices and services, minimizing the risk of unauthorized exploitation.
- Stay informed about security advisories and updates from Cisco and other relevant sources to promptly address emerging threats and vulnerabilities.
- In case of any incident, please report to this office, through PTA CERT Portal and email.