Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No: 146 **27-09-2021**

Name: Critical Vulnerability in CISCO IOS XE Software

Threat Classification: Remote Code Execution

Affected Products:

- Catalyst 9800 Embedded Wireless Controller for Catalyst 9300, 9400, and 9500 Series Switches
- Catalyst 9800 Series Wireless Controllers
- Catalyst 9800-CL Wireless Controllers for Cloud
- Embedded Wireless Controller on Catalyst Access Points

Summary:

Critical vulnerabilities are found in CISCO affecting the components in its IOS XE **internetworking operating system** powering routers and wireless controllers, or products running with a specific configuration. It affects the Cisco Catalyst 9000 Family Wireless Controllers that includes the enterprise-class Catalyst 9800-CL Wireless Controllers for Cloud. The vulnerability is due to a logic error that occurs during the validation of CAPWAP packets. An attacker could exploit this vulnerability by sending a crafted CAPWAP packet to an affected device. This vulnerability could be exploited remotely by an unauthenticated attacker to run arbitrary code with root privileges and can cause a **denial-of-service** (**DoS**) condition.

Severity	**Critical**
Attack Vector	Network
Privileges required	None

For further details, please visit following link:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ewlc-capwap-rce-LYgj8Kf

Recommendations:

- Please visit the website link for remediation and workarounds for the aforementioned vulnerabilities:
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ewlc-capwap-rce-LYgj8Kf#fs
- It is recommended to **update** all your software's.
- When considering software upgrades, customers are advised to regularly consult the advisories for Cisco products, which are available from the Cisco Security Advisories page, to determine exposure and a complete upgrade solution.
- Use licensed antivirus and regularly obtain its latest updates with its real-time scanning capabilities enabled.
- Only use licensed software and avoid download/use of cracked and pirated software.
- Designate a PoC from your security / Network team (if yet not designated), for seeking assistance and reporting security issues.
- In case of any incident, please report to this office.