PTA Security Advisory-No: 55

07-October-2019

Threat Classification: Buffer Overflow Vulnerability

Name: CISCO IOS XE Software FTP ALG for NAT, NAT64 and ZBFW Denial of Service (CVE-2019-12655)

Affected Systems: Affects the following product of CISCO:

- **Cisco IOS XE Software**

This vulnerability affects the devices which are running a vulnerable release of Cisco IOS XE Software with NAT, NAT64 or ZBFW(Zone-Based Policy Firewall) when FTP inspection is enabled.

Summary: In Cisco IOS XE Software, the FTP application layer gateway (ALG) functionality which is used by Network Address Translation (NAT), NAT IPv6 to IPv4 (NAT64) and the Zone-Based Policy Firewall (ZBFW) has a vulnerability that allows an unauthenticated remote attacker to reload the affected device, resulting in a Denial of Service attack. This is due to buffer overflow that occurs when the affected device inspects certain FTP traffic. The attacker exploits this vulnerability by performing a specific FTP transfer through the device.

Attack Severity	HIGH
Attack Vector	Network
Attack Type	Denial of Service
Privileges Required	None

- For more information about which Cisco IOS XE Software releases are vulnerable, please visit following link: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925-ftp#fs

- To help customers determine their exposure to vulnerabilities and the earliest release that fixes the vulnerabilities in Cisco IOS XE Software, Cisco provides a tool, the Cisco IOS Software Checker, that identifies any Cisco Security Advisories that impact a specific software.

Wordarounds: Administrators can disable the FTP ALG function by using the following commands on the affected device until the software upgrade is performed:

- Administrators can use the **no ip nat service ftp** command in global configuration mode to disable the use of NAT ALG for FTP.
- Administrators can use the **no nat64 service ftp** command in global configuration mode to disable the use of NAT64 ALG for FTP.
- Remove the commands **match protocol ftp** and **match protocol ftps** from the inspection class map to disable the use of FTP inspection in the ZBFW.

Note: Disable the FTP ALG function only if it is not required in your environment.

Recommendations:

- Update from following official Cisco IOS XE Software Releases to fix the aforementioned vulnerabilities:
  - https://tools.cisco.com/security/center/softwarechecker.x
- Whenever required, run software with minimal access rights and privileges.
- 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.