PTA Security Advisory-No: 57

28-October-2019

Threat Classification: Denial of Service Vulnerability

Name:

a. CISCO ASA and Firepower Threat Defense (FTD) Software with FTP Inspection Denial of Service (DOS) Vulnerability (CVE-2019-12673)

b. CISCO ASA and Firepower Threat Defense (FTD) Software with Open Shortest Path First (OSPF) LSA Processing Denial of Service (DOS) Vulnerability (CVE-2019-12676)

Affected Systems: Affects the following products of CISCO:

a. Vulnerable release of ASA or FTD Software **with FTP inspection configured**.

b. Vulnerable release of ASA or FTD Software **configured to support OSPF Routing**.

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

Summary:

a. **Cisco ASA & FTD Software with FTP inspection**: A vulnerability in the FTP inspection engine of ASA and FTD software could allow an attacker to cause a DOS attack on the affected device due to insufficient validation of the FTP data by sending malicious FTP traffic through the affected device. Further details are available at:

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-asa-dos

b. **Cisco ASA & FTD Software configured with OSPF Routing**: A vulnerability in OSPF implementation of Cisco ASA and FTD Software could allow an attacker to cause a reload to the affected device resulting in a DOS attack. This vulnerability exists because the affected software improperly parses certain options in OSPF link-state advertisement (LSA) type 11 packets. Further details are available at:

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-asa-ospf-lsa-dos

Fixed Releases:

a. For CISCO ASA or FTD with FTP Inspection fixed releases, please use following link:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-asa-ospf-lsa-dos#fs

b. For CISCO ASA or FTD with OSPF routing fixed releases, please use following link:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-asa-ospf-lsa-dos

Recommendations:

- Update or upgrade software from following official Cisco website link for ASA and FTD Software releases to fix the aforementioned vulnerabilities:

  a. **For FTP Inspection DOS Vulnerability**:
  https://software.cisco.com/download/home/284143092/type/280775065/release

  b. **For OSPF LSA Processing DOS Vulnerability**:
  https://software.cisco.com/download/home/286271172/type/286306337/release

- In all cases, ensure that devices to be upgraded to new release meet the requirements set by the vendor.
- 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.