Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No: 079 29-April-2020

Name: Juniper Networks Junos OS Multiple IPSec AH Vulnerabilities

Threat Classification: Denial of Service (DoS)

Affected Systems: Affects the following Juniper Networks Junos OS versions:

- 15.1, 15.1X49, 15.1X53.
- 16.1, 16.2.
- 17.1, 17.2, 17.2X75, 17.3, 17.4.
- 18.1, 18.2, 18.2X75, 18.3, 18.4.
- 19.1, 19.2, 19.3.

Summary:

These issues allow an attacker to potentially be able to take control of the device by sending a specifically crafted IP packet or by sending an arbitrary packet to the device that may lead to a system crash or Denial of Service (DoS). These issues affect systems configured for IPsec when the Authentication Header (AH) protocol is used.

Severity Level	**Critical**
Attack Vector	Network
Privileges Required	None

Multiple vulnerabilities that affect FreeBSD's implementation of IPSec's AH protocol have been fixed in Juniper Networks Junos OS.

For further details, please visit following vendor official link:

https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11016&cat=SIRT_1&actp=LIST

Recommendations:

- Please visit the following official website link for the software releases, patches and updates for the remediation of aforementioned vulnerabilities:
  - https://www.juniper.net/support/downloads/
- In all cases, ensure the availability of stable version, before upgrade, by the relevant vendor.
- In all cases, also ensure that devices to be upgraded to new release meet the requirements set by the vendor.
- Whenever required, access the system 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.