

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

<http://www.us-cert.gov/tlp/>

DATE(S) ISSUED:

10/15/2020

SUBJECT:

A Vulnerability in Juniper Junos OS Could Allow for Denial of Service

OVERVIEW:

A vulnerability has been discovered in Juniper Junos OS, which could allow for denial of service. Junos OS is a FreeBSD-based operating system used in Juniper Networks routers. This vulnerability specifically affects MX Series routers and EX9200 series switches with Trio-based PFEs configured with IPv6 Distributed Denial of Service (DDoS) protection mechanism enabled. An attacker can exploit this issue to disrupt network protocol operations or interrupt traffic. Successful exploitation of this vulnerability could result in denial of service conditions.

THREAT INTELLIGENCE:

There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED

This issue affects Juniper Networks Junos OS on MX series and EX9200 Series:

- 17.2 versions prior to 17.2R3-S4;
- 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110;
- 17.3 versions prior to 17.3R3-S8;
- 17.4 versions prior to 17.4R2-S11, 17.4R3-S2;
- 18.2 versions prior to 18.2R2-S7, 18.2R3, 18.2R3-S3;
- 18.2X75 versions prior to 18.2X75-D30;
- 18.3 versions prior to 18.3R2-S4, 18.3R3-S2.

RISK:

Government:

- Large and medium government entities: **HIGH**
- Small government entities: **HIGH**

Businesses:

- Large and medium business entities: **HIGH**
- Small business entities: **HIGH**

Home Users: LOW

TECHNICAL SUMMARY:

A vulnerability has been discovered in Juniper Junos OS, which could allow for denial of service. This vulnerability specifically affects MX Series routers and EX9200 series switches with Trio-based PFEs configured with IPv6 Distributed Denial of Service (DDoS) protection mechanism enabled. The IPv6 DDoS protection mechanism allows the device to continue to function while it is under DDoS attack, protecting both the Routing Engine (RE) and the Flexible PIC Concentrator (FPC) during the DDoS attack. An attacker can exploit this issue to disrupt network protocol operations or interrupt traffic by overwhelming the Routing Engine (RE) and/or the Flexible PIC Concentrator (FPC). Successful exploitation of this vulnerability could result in denial of service conditions.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Juniper to vulnerable systems immediately after appropriate testing.
- Disable all unnecessary services.
- Restrict access to devices and applications from only authorized users and hosts.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:**Juniper:**

<https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11062>

CVE:

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1665>

TLP: WHITE

Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

<http://www.us-cert.gov/tlp/>