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

https://www.cisa.gov/tlp

Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

DATE(S) ISSUED:

04/15/2021

SUBJECT:

A Vulnerability in Juniper Junos OS Could Allow for Remote Code Execution

OVERVIEW:

A vulnerability has been discovered in Juniper Junos OS that could allow for remote code execution. Junos OS is a single network operating system providing a common language across Juniper's routing, switching and security devices. This vulnerability specifically affects the overlayd service of Juniper Networks Junos OS. The overlayd daemon handles Overlay OAM packets, such as ping and traceroute, sent to the overlay. The service runs as root by default and listens for UDP connections on port 4789. This issue results from improper buffer size validation, which can lead to a buffer overflow. Unauthenticated attackers can send specially crafted packets to trigger this vulnerability, resulting in possible remote code execution.

Successful exploitation of this vulnerability could allow for remote code execution. Depending on the privileges associated with the application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Applications that are configured to have fewer user rights on the system could be less impacted than those that operate with administrative user rights.

THREAT INTELLIGENCE:

There are currently no reports of this vulnerability being exploited in the wild.

SYSTEMS AFFECTED:

- 15.1X49 versions prior to 15.1X49-D240 on SRX Series;
- 15.1 versions prior to 15.1R7-S9;
- 17.3 versions prior to 17.3R3-S11;
- 17.4 versions prior to 17.4R2-S13, 17.4R3-S4;
- 18.1 versions prior to 18.1R3-S12;
- 18.2 versions prior to 18.2R2-S8, 18.2R3-S7;
- 18.3 versions prior to 18.3R3-S4;
- 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7;
- 19.1 versions prior to 19.1R2-S2, 19.1R3-S4;
- 19.2 versions prior to 19.2R1-S6, 19.2R3-S2;
- 19.3 versions prior to 19.3R3-S1;
- 19.4 versions prior to 19.4R2-S4, 19.4R3-S1;
- 20.1 versions prior to 20.1R2-S1, 20.1R3;

- 20.2 versions prior to 20.2R2, 20.2R2-S1, 20.2R3;
- 20.3 versions prior to 20.3R1-S1.

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
A vulnerability has been discovered in Juniper Junos OS that could allow for remote code execution. Juniper Junos is prone to a buffer-overflow vulnerability because it fails to properly validate the buffer size. Specifically, this issue exists in the 'overlayd' service. A remote unauthenticated attacker can exploit this issue by sending a specially-crafted packets to the affected device. An attacker can exploit this issue to execute arbitrary code within the context of the affected system. Failed exploits may result in denial-of-service conditions.

Successful exploitation of this vulnerability could allow for remote code execution. Depending on the privileges associated with the application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Applications that are configured to have fewer user rights on the system could be less impacted than those that operate with administrative user rights.

RECOMMENDATIONS:
The following actions should be taken:
- Block external access at the network boundary, unless external parties require service.
- If global access isn't needed, filter access to the affected computer at the network boundary. Restricting access to only trusted computers and networks might greatly reduce the likelihood of successful exploits.
- Run all software as a nonprivileged user with minimal access rights. To mitigate the impact of a successful exploit, run the affected application as a user with minimal access rights.
- Deploy network intrusion detection systems to monitor network traffic for malicious activity.
- Deploy NIDS to detect and block attacks and anomalous activity such as requests containing suspicious URI sequences. Since the webserver may log such requests, review its logs regularly.
- Implement multiple redundant layers of security. Since this issue may be leveraged to execute code, we recommend memory-protection schemes, such as nonexecutable stack/heap configurations and randomly mapped memory segments. This tactic may complicate exploit attempts of memory-corruption vulnerabilities.

REFERENCES:
CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-0254

Juniper:

https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11147

TLP: WHITE

https://www.cisa.gov/tlp

Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.