

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

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

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

DATE(S) ISSUED:

12/18/2015

12/22/2015 - UPDATED

SUBJECT:

Multiple Vulnerabilities in Juniper ScreenOS Could Allow Unauthorized, Remote Access or Remote Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in Juniper ScreenOS that could allow unauthorized, remote administrative access to the device, the ability to decrypt VPN connections, or cause denial of service conditions which could lead to remote code execution. ScreenOS is the operating system used by NetScreen devices. Typical NetScreen devices are Juniper VPN security products and high-performance firewalls. Successful exploitation could lead to remote, administrative access of an impacted NetScreen device, allow for the decryption of VPN connections, resulting in the exposure of secured traffic, and/or result in a system crash that could lead to remote code execution.

THREAT INTELLIGENCE:

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

Two of these vulnerabilities are due to the addition of unauthorized code in ScreenOS. No further information regarding the source of the unauthorized code is currently available.

December 22 - UPDATED THREAT INTELLIGENCE:

A password that will allow administrative access for specific vulnerable versions of ScreenOS have been publically released via a Rapid7 blog post. An increase in scanning attempts for vulnerable systems have been observed from open-source reports.

SYSTEMS AFFECTED:

- ScreenOS 6.2.0r15 through 6.2.0r18
- ScreenOS 6.3.0r12 through 6.3.0r20

December 22 – UPDATED SYSTEMS AFFECTED (exploitable by the password identified in the blog post)

:

- ***ScreenOS 6.3.0r17, 6.3.0r18, 6.3.0r19, and 6.3.0r20***

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: N/A

TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in Juniper ScreenOS that could allow unauthorized, remote administrative access to the device, the ability to decrypt VPN connections, or cause denial of service conditions which could lead to remote code execution. Successful exploitation could lead to remote, administrative access of an impacted NetScreen device, allow for the decryption of VPN connections, resulting in the exposure of secured traffic, and/or result in a system crash that could lead to remote code execution.

The first vulnerability identified could lead to remote administrative access (via SSH or Telnet) of a NetScreen device, resulting in the complete compromise of the impacted system. When exploited the vulnerability generates a log file containing an entry that user 'system' had logged on followed by the password authentication for a username.

Example:

*Normal login by user **username1**:*

*2015-12-17 09:00:00 system warn 00515 Admin user **username1** has logged on via SSH from ...*

2015-12-17 09:00:00 system warn 00528 SSH: Password authentication successful for admin user 'username1' at host ...

*Compromised login by user **username2**:*

*2015-12-17 09:00:00 system warn 00515 Admin user **system** has logged on via SSH from ...*

2015-12-17 09:00:00 system warn 00528 SSH: Password authentication successful for admin user 'username2' at host ...

The second vulnerability could allow a knowledgeable attacker, who can monitor VPN traffic, the ability to decrypt VPN connections in a man-in-the-middle scenario. There is no way to detect if this vulnerability was exploited.

The third vulnerability could allow an attacker to cause a denial of service condition by using the vulnerable SSH packet handling mechanism present in Juniper ScreenOS when ssh-pka is configured and enabled on the firewall. The resulting system crash could lead to remote code execution.

December 22 - UPDATED TECHNICAL SUMMARY:

The password provided by the Rapid7 security group allows an attacker to remotely login as an administrator over SSH and Telnet using any username.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Juniper to vulnerable systems immediately after appropriate testing.
- Limit management access to the device only from trusted, internal, administrative networks or hosts and/or restrict access to device management services (via SSH and Telnet) to authorized hosts.
- Review log files for 'system' login attempts.
- Monitor systems for any signs of anomalous activity.

REFERENCES:

Juniper:

<http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10713&actp=search>

<http://forums.juniper.net/t5/Security-Incident-Response/Important-Announcement-about-ScreenOS/ba-p/285554>

http://kb.juniper.net/InfoCenter/index?page=content&channel=SECURITY_ADVISORIES

<http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10712&actp=RSS>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7754>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7755>

December 22 – UPDATED REFERENCES:

Rapid7

<https://community.rapid7.com/community/infosec/blog/2015/12/20/cve-2015-7755-juniper-screenos-authentication-backdoor>

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

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