TLP: WHITE
MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER:
2018-004

DATE(S) ISSUED:
01/17/2018

SUBJECT:
Multiple Vulnerabilities in Juniper Products Could Allow for Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Juniper products, the most severe of which could allow for remote code execution. Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution within the context of the application, an attacker gaining the same privileges as the logged-on user, or the bypassing of security restrictions. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:
These updates also include patches to Juniper systems for the Spectre and Meltdown vulnerabilities. There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- CTP Series
- CTPView Prior to version 7.1R2, 7.3R3 and 7.4R1
- Multiple Junos OS 12.1x46 versions
- Multiple Junos OS 12.3, 12.3R, 12.3R12, 12.3X48 versions
- Multiple Junos OS 14.1, 14.1X53 versions
- Multiple Junos OS 14.2 versions
- Multiple Junos OS 15.1, 15.1R5-S4, 15.1R5-S5; 15.1R6, 15.1X49, 15.1X53 versions
- Multiple Junos OS 16.1, 16.1X65 versions
- Multiple Junos OS 16.2 versions
- Multiple Junos OS 17.1 versions
- Multiple Junos OS 17.2, 17.2X75 versions
- Junos OS based platforms
- Junos Space appliance
- Junos Space Prior to version 17.2R1
- NSMXpress/NSM3000/NSM4000 appliances
- Qfabric Director
- ScreenOS prior to 6.3.0r25
- Security Director and Log Collector Prior to version 17.2R1
- SRC/C Series
- STRM/Juniper Secure Analytics (JSA) appliances

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:
Multiple vulnerabilities have been discovered in Juniper products, the most severe of which could allow for arbitrary code execution. Details of these vulnerabilities are as follows:

- Modern microprocessors that implement speculative execution of instructions are susceptible to a new class of cache timing attacks being called "Meltdown" and "Spectre". These vulnerabilities could allow an attacker to read privileged memory which may contain sensitive information such as passwords or encryption keys. (CVE-2017-5715, CVE-2017-5753, CVE-2017-5754)
- A remote, unauthenticated attacker may be able to execute code by exploiting a use-after-free defect found in older versions of PHP through injection of crafted data via specific PHP URLs within the context of the J-Web process. (CVE-2018-0001)
- On SRX Series and MX Series devices with a Service PIC with any ALG enabled, a crafted TCP/IP response packet processed through the device results in memory corruption leading to a flowd daemon crash. Sustained crafted response packets lead to repeated crashes of the flowd daemon which results in an extended Denial of Service condition. (CVE-2018-0002)
- A specially crafted MPLS packet received or processed by the system, on an interface configured with MPLS, will store information in the system memory. Subsequently, if this stored information is accessed, this may result in a kernel crash leading to a denial of service. (CVE-2018-0003)
- A sustained sequence of different types of normal transit traffic can trigger a high CPU consumption denial of service condition in the Junos OS register and schedule software interrupt handler subsystem when a specific command is issued to the device. This affects one or more threads and conversely one or more running processes running on the system. Once this occurs, the high CPU event(s) affects either or both the forwarding and control plane. As a result of this condition the device can become inaccessible in either or both the control and forwarding plane and stops forwarding traffic until the device is rebooted. For network designs utilizing layer 3 forwarding agents or other ARP through layer 3 technologies, the score is slightly higher. The issue will reoccur after reboot upon receiving further transit traffic. If the following entry exists in the RE message logs then this may indicate the issue is present. This entry may or may not appear when this issue occurs. (CVE-2018-0004)
- QFX and EX Series switches configured to drop traffic when the MAC move limit is exceeded will forward traffic instead of dropping traffic. This can lead to denials of services or other unintended conditions. (CVE-2018-0005)
- A high rate of VLAN authentication attempts sent from an adjacent host on the local broadcast domain can trigger high memory utilization by the BBE subscriber management daemon (bbe-smgd), and lead to a denial of service condition. The issue was caused by attempting to process an unbounded number of pending VLAN authentication requests, leading to excessive memory allocation. This issue only affects devices configured for DHCPv4/v6 over AE auto-sensed VLANs, utilized in Broadband Edge (BBE) deployments. Other configurations are unaffected by this issue. (CVE-2018-0006)
- An unauthenticated root login may allow upon reboot when a commit script is used. A commit script allows a device administrator to execute certain instructions during commit, which is configured under the [system scripts commit] stanza. Certain commit scripts that work without a problem during normal commit may cause unexpected behavior upon reboot which can leave the system in a state where root CLI login is allowed without a password due to the system reverting to a "safe mode" authentication state. Lastly, only logging in physically to the console port as root, with no password, will work. (CVE-2018-0008)
- On Juniper Networks SRX series devices, firewall rules configured to match custom application UUIDs starting with zeros can match all TCP traffic. Due to this issue, traffic that should have been blocked by other rules is permitted to flow through the device resulting in a firewall bypass condition. (CVE-2018-0009)
- Remote network based attackers can cause the OpenSSH server on Junos OS to allocate an excessive amount of memory. This can potentially create a denial of service condition for the device. The issue only occurs if SSH is enabled. An attacker must be able to first establish a connection to the SSH service on the device. This vulnerability cannot be triggered from hosts or networks that cannot reach the SSH port on the device. (CVE-2016-8858)

- Multiple vulnerabilities have been resolved in the Junos Space 17.2R1 release, including updates to third party software found within Junos Space. (CVE-2017-14106, CVE-2017-1000111, CVE-2016-8655, CVE-2018-1000112, CVE-2015-7501, CVE-2015-5304, CVE-2016-2141, CVE-2015-5174, CVE-2017-5645, CVE-2017-5664, CVE-2015-5188, CVE-2015-5220, CVE-2015-7236, CVE-2016-8743, CVE-2017-3167, CVE-2017-3169, CVE-2017-7668, CVE-2017-7679, CVE-2017-9788, CVE-2017-9798, CVE-2018-0011, CVE-2018-0012, CVE-2018-0013, CVE-2017-12172, CVE-2017-15098)
- CTPView releases 7.1R2, 7.3R3 and 7.4R1 address multiple Linux kernel vulnerabilities in prior releases. (CVE-2017-6074, CVE-2017-2634)
- Juniper Networks ScreenOS devices do not pad Ethernet packets with zeros, and thus some packets can contain fragments of system memory or data from previous packets. This issue is often detected as CVE-2003-0001. The issue affects all versions of Juniper Networks ScreenOS prior to 6.3.0r25. Juniper SIRT is not aware of any malicious exploitation of this vulnerability. This issue was discovered during an external security research. This issue is also known as Etherleak. (CVE-2003-0001, CVE-2018-0014)

Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution within the context of the application, an attacker gaining the same privileges as the logged-on user, or the bypassing of security restrictions. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:
We recommend the following actions be taken:

- Apply appropriate patches provided by Juniper to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- 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=JSA10842&cat=SIRT_1&actp=LIST
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10828&cat=SIRT_1&actp=LIST
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10829&cat=SIRT_1&actp=LIST
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10831&cat=SIRT_1&actp=LIST
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10832&cat=SIRT_1&actp=LIST
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10833&cat=SIRT_1&actp=LIST
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10834&cat=SIRT_1&actp=LIST
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10835&cat=SIRT_1&actp=LIST
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10836&cat=SIRT_1&actp=LIST
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10837&cat=SIRT_1&actp=LIST
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10838&cat=SIRT_1&actp=LIST
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10839&cat=SIRT_1&actp=LIST
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10839&cat=SIRT_1&actp=LIST
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10841&cat=SIRT_1&actp=LIST

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1000111
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3169
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5174
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5220
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5664

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5715
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5753
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0013
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2634
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5188
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5754
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0001
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0001
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0002
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0014
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-12172
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14106
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-15098
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2141
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3167
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5304
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5645
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6074
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7236
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7501
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7668
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7679
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8655
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9798
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0003
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0004
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0005
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0006
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0008
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0009
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0011
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0012
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1000112
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8743
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8858
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-9788

24x7 Security Operations Center
Multi-State Information Sharing and Analysis Center (MS-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722