TLP: WHITE
MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER: 2018-041

DATE(S) ISSUED: 04/13/2018

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 result in the attacker gaining control of the affected system. Depending on the privileges associated with this application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

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

SYSTEMS AFFECTED:
- All products and platforms running Junos OS

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

Businesses:
- Large and medium government entities: **High**
- Small government entities: **High**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Juniper products, the most severe of which could allow for remote code execution. Details of these vulnerabilities are as follows:
- A Junos device with VPLS routing-instances configured on one or more interfaces may be susceptible to an mbuf leak when processing a specific MPLS packet. The successful exploitation of this vulnerability could cause approximately 1 mbuf to be leaked per each packet processed (CVE-2018-0022).
- Juniper devices configured with short MacSec keys are at risk of man-in-the-middle attacks. The successful exploitation of this vulnerability could allow an attacker to discover the secret passphrases configured for these keys through dictionary-based and brute-force-based attacks using spoofed packets (CVE-2018-0021).
- Multiple vulnerabilities in stunnel software included with Junos OS have been resolved by upgrading stunnel to 5.38. Stunnel is used for providing SSL/TLS protection to Junos XML protocol server (xnm-ssl). These issues only affect devices where xnm-ssl is configured (CVE-2014-0016, CVE-2008-2420).
- A remote, network based attacker may be able to cause the mib2d process to crash resulting in a denial-of-service condition for the SNMP subsystem. This vulnerability only affects systems with SNMP mib2d enabled, meaning the successful exploitation of this vulnerability could disrupt network monitoring via SNMP, but will not impact routing, switching, or firewall functionalities (CVE-2018-0019).
- A remote, unauthenticated attacker may be able to cause a kernel crash or execute code by sending a specially crafted Connectionless Network Protocol (CLNP) packet to an interface IP address of a Junos OS device (CVE-2018-0016).
- An extended denial-of-service condition may be experienced by devices that receive repeated malformed BGP UPDATES. These malformed BGP Updates cause the routing process daemon to crash and restart. This vulnerability only impacts Junos OS 13.2R1 and later releases (CVE-2018-0020).

Successful exploitation of the most severe of these vulnerabilities could result in the attacker gaining control of the affected system. Depending on the privileges associated with this application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative 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=JSA10855&cat=JUNOS&actp=LIST
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10854&cat=JUNOS&actp=LIST
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10852&cat=JUNOS&actp=LIST
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10848&cat=JUNOS&actp=LIST
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10847&cat=JUNOS&actp=LIST
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10844&cat=JUNOS&actp=LIST

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2420
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0016
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0016
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0019
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0020
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0021
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0022

24×7 Security Operations Center
Multi-State Information Sharing and Analysis Center (MS-ISAC)
Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722