computer emergency response team
CERT-EU
for the EU institutions, bodies and agencies

CERT-EU Security Advisory 2018-017

Juniper JunOS Multiple Vulnerabilities

July 13, 2018 — v1.0

History:

- *13/07/2018 — v1.0 – Initial publication*

Summary

On the 12th of July 2018, Juniper has released updates to address several vulnerabilities affecting JunOS products. [1] A remote attacker can exploit those vulnerabilities in order to trigger privilege escalation, denial of service, firewall rule bypass, security restriction bypass and sensitive information disclosure on the targeted system. An exploit is available for the privilege escalation vulnerability (CVE-2018-0024). [2]

Technical Details

Vulnerabilities impact is presented below.

Critical

- RPD daemon crashes due to receipt of crafted BGP NOTIFICATION messages (CVE-2018-0037)
- Junos Space: Multiple vulnerabilities resolved in 18.1R1 release
- Junos OS: cURL: Multiple vulnerabilities in multiple cURL versions

High

- Privilege escalation vulnerability exists where authenticated users with shell access can become root (CVE-2018-0024)
- Receipt of malformed RSVP packet may lead to RPD denial of service (CVE-2018-0027)
- MPC7/8/9, PTX-FPC3 (FPC-P1, FPC-P2) and PTX1K: Line card may crash upon receipt of specific MPLS packet (CVE-2018-0030)
- RPD crash when receiving a crafted BGP UPDATE (CVE-2018-0032)

Medium

- FreeBSD-SA-15:24.rpcbind : rpcbind(8) remote denial of service
- SRX Series: Credentials exposed when using HTTP and HTTPS Firewall Pass-through User Authentication (CVE-2018-0025)

- Stateless IP firewall filter rules stop working as expected after reboot or upgrade (CVE-2018-0026)
- Kernel crash (vmcore) during broadcast storm after enabling 'monitor traffic interface fxp0' (CVE-2018-0029)
- Receipt of specially crafted UDP packets over MPLS may bypass stateless IP firewall rules (CVE-2018-0031)
- A malicious crafted IPv6 DHCP packet may cause the JDHCPD daemon to core (CVE-2018-0034)
- QFX5200 and QFX10002: Unintended ONIE partition was shipped with certain Junos OS .bin and .iso images (CVE-2018-0035)

Products Affected

Due to the fact that multiple products are affected, below you will find only products families. For more details please consult Juniper Security Advisories and Alerts web site [1].

- Junos OS 12.1 to 18.2
- EX Series
- QFX3500
- QFX3600
- QFX5100
- QFX5200
- QFX10002
- SRX Series
- JunOS Space

Recommendations

Upgrade products based on Juniper recommendations [1].

Workarounds

Due to the large number of products affected please consult the specific vulnerable product workaround, if any [1].

References

[1] https://kb.juniper.net/InfoCenter/index?page=content&channel=SECURITY_ADVISORIES

[2] https://0day.city/cve-2018-0024.html