مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Juniper Security Updates

Tracking #:432315964

Date:20-06-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Juniper Networks released security updates to patch multiple vulnerabilities in Juniper Secure Analytics.

TECHNICAL DETAILS:

The Juniper Networks released security updates for Juniper Secure Analytics software that contains multiple critical vulnerabilities. These vulnerabilities can lead to local privilege escalation, denial of service, and information disclosure.

Severity: Critical
Severity Assessment (CVSS) Score: 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Notable Vulnerabilities Addressed:

CVE ID	CVSS Score	Description
CVE-2019-19012	9.8	An integer overflow in the search_in_range function in regexec.c in Oniguruma 6.x before 6.9.4_rc2 leads to an out-of-bounds read, in which the offset of this read is under the control of an attacker. (This only affects the 32-bit compiled version). Remote attackers can cause a denial-of-service or information disclosure, or possibly have unspecified other impact, via a crafted regular expression.
CVE-2019-13224	9.8	A use-after-free in onig_new_deluxe() in regext.c in Oniguruma 6.9.2 allows attackers to potentially cause information disclosure, denial of service, or possibly code execution by providing a crafted regular expression. The attacker provides a pair of a regex pattern and a string, with a multi-byte encoding that gets handled by onig_new_deluxe(). Oniguruma issues often affect Ruby, as well as common optional libraries for PHP and Rust.
CVE-2023-5178	9.8	A use-after-free vulnerability was found in drivers/nvme/target/tcp.c` in `nvmet_tcp_free_crypto` due to a logical bug in the NVMe/TCP

		subsystem in the Linux kernel. This issue may allow a malicious user to cause a use-after-free and double-free problem, which may permit remote code execution or lead to local privilege escalation.

Affected Versions:

- All versions prior to 7.5.0 UP8 and 7.5.0 UP8 IF02

Fixed Version:

- Juniper Networks Juniper Secure Analytics 7.5.0 UP8

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates released by Juniper Networks.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://supportportal.juniper.net/s/article/On-Demand-JSA-Series-Multiple-vulnerabilities-resolved-in-Juniper-Secure-Analytics-in-7-5-0-UP8-IF03?language=en_US