مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates-Juniper Networks

Tracking #:432316383

Date:10-10-2024

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

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

TECHNICAL DETAILS:

Juniper Networks has released security updates to address multiple vulnerabilities in its products. These vulnerabilities, if exploited, could lead to serious consequences such as remote code execution, denial-of-service (DoS) attacks, and unauthorized access.

Vulnerabilities Details:

Description	Severity
JSA86686 : On Demand: JSA Series: Multiple vulnerabilities resolved in Juniper Secure Analytics in 7.5.0 UP9 IF03	Critical
JSA88135 : 2024-10 Security Bulletin: Junos OS: Multiple vulnerabilities in OSS component nginx resolved	Critical
JSA88100 : 2024-10 Security Bulletin: Junos OS and Junos OS Evolved: With BGP traceoptions enabled, receipt of specifically malformed BGP update causes RPD crash (CVE-2024-39516)	High
JSA88099 : 2024-10 Security Bulletin: Junos OS and Junos OS Evolved: With BGP traceoptions enabled, receipt of specially crafted BGP update causes RPD crash (CVE-2024-39515)	High
JSA88124 : 2024-10 Security Bulletin: Junos OS: SRX Series, QFX Series, MX Series and EX Series: Receiving specific HTTPS traffic causes resource exhaustion (CVE-2024-47497)	High
JSA88112 : 2024-10 Security Bulletin: Junos OS Evolved: Multiple vulnerabilities resolved in c-ares 1.18.1	High
JSA88134 : 2024-10 Security Bulletin: Junos OS: SRX5000 Series: Receipt of a specific malformed packet will cause a flowd crash (CVE-2024-47504)	High
JSA88120 : 2024-10 Security Bulletin: Junos OS: J-Web: Multiple vulnerabilities resolved in PHP software.	High
JSA88102 : 2024-10 Security Bulletin: Junos OS and Junos OS Evolved: When BGP nexthop traceoptions is enabled, receipt of specially crafted BGP packet causes RPD crash (CVE-2024-39525)	High
JSA88108 : 2024-10 Security Bulletin: Junos OS and Junos OS Evolved: cRPD: Receipt of crafted TCP traffic can trigger high CPU utilization (CVE-2024-39547)	High
JSA88132 : 2024-10 Security Bulletin: Junos OS Evolved: TCP session state is not always cleared on the Routing Engine (CVE-2024-47502)	High
JSA88129 : 2024-10 Security Bulletin: Junos OS and Junos OS Evolved: In a BMP scenario receipt of a malformed AS PATH attribute can cause an RPD core (CVE-2024-47499)	High
JSA88110 : 2024-10 Security Bulletin: Junos Space: Remote Command Execution (RCE) vulnerability in web application (CVE-2024-39563)	High
JSA88116 : 2024-10 Security Bulletin: Junos OS and Junos OS Evolved: Receipt of a specific malformed BGP path attribute leads to an RPD crash (CVE-2024-47491)	High
JSA88115 : 2024-10 Security Bulletin: Junos OS Evolved: ACX 7000 Series: Receipt of specific transit MPLS packets causes resources to be exhausted (CVE-2024-47490)	High
JSA88210 : 2024-09-30 Out of Cycle Security Advisory: Multiple Products: RADIUS protocol susceptible to forgery attacks (Blast-RADIUS) (CVE-2024-3596)	High
JSA83011 : 2024-07 Security Bulletin: Junos OS and Junos OS Evolved: Receipt of malformed BGP path attributes leads to RPD crash (CVE-2024-39549)	High
JSA87479 : Mist: RADIUS Protocol Vulnerability (Blast-RADIUS) (CVE-2024-3596)	High

Note: Refer to Juniper Networks advisory for CVEs, fixed versions, and more information.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates recently 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:

- http://supportportal.juniper.net/s/global-search/%40uri?language=en_US#sort=%40sfcec_community_publish_date_formula__c%20descending&f:ctype=[Security%20Advisories]&f:slevel=[Critical,High]