مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Red Hat - Vulnerability in NetworkManager-libreswan

Tracking #:432316430
Date:23-10-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in the libreswan client plugin for NetworkManager, which could potentially allow attackers to gain root privileges on Red Hat Enterprise Linux systems.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-9050**
- CVSS v3.1 Base Score: 7.8
- Severity**:** High
- **Affected Component:** NetworkManager-libreswan
- The vulnerability arises from improper sanitization of VPN configurations. The plugin fails to escape special characters in key-value pairs, leading to potential manipulation of the 'leftupdownkey' parameter. This parameter executes a command as a callback, allowing attackers to inject malicious code and gain unauthorized access.
- Local attackers could exploit this vulnerability to escalate their privileges and execute arbitrary code with root privileges.

Mitigations:

Red Hat has released security updates to address this vulnerability in the following products:

- Red Hat Enterprise Linux 9.0 Update Services for SAP Solutions
- Red Hat Enterprise Linux 7.7 Advanced Update Support

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates recently released by Red Hat.

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://nvd.nist.gov/vuln/detail/CVE-2024-9050