مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in Cisco Small Business Routers

Tracking #:432316367

Date:07-10-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Cisco has identified multiple vulnerabilities in its Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers.

TECHNICAL DETAILS:

Cisco has identified multiple vulnerabilities in its Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers. These vulnerabilities could allow authenticated remote attackers to escalate privileges and execute arbitrary commands on affected devices. Given that these products have reached their End-of-Software-Maintenance deadlines, no patches or workarounds are available, posing a significant risk to small business networks.

Details of Vulnerabilities:

1. CVE-2024-20393 – Privilege Escalation Vulnerability
    - **Severity**: High (CVSS Score: 8.8)
    - **Description**: This vulnerability allows an authenticated remote attacker to escalate privileges from a guest account to an admin account via the web-based management interface. The flaw arises from improper disclosure of sensitive information.
    - **Exploitation**: Attackers can exploit this vulnerability by sending crafted HTTP input to the device, gaining unauthorized administrative control.
2. CVE-2024-20470 – Remote Command Execution Vulnerability
    - **Severity**: Medium (CVSS Score: 4.7)
    - **Description**: This vulnerability enables attackers with valid admin credentials to execute arbitrary code on the underlying operating system due to insufficient validation of user-supplied input.
    - **Exploitation**: By sending crafted HTTP input, an attacker could execute commands with root privileges.

Affected Devices:

The following devices are vulnerable:

- RV340 Dual WAN Gigabit VPN Routers
- RV340W Dual WAN Gigabit Wireless-AC VPN Routers
- RV345 Dual WAN Gigabit VPN Routers
- RV345P Dual WAN Gigabit PoE VPN Routers

RECOMMENDATIONS:

- **Disable Remote Management**: Ensure that the remote management feature is disabled to reduce exposure.
- **Upgrade Devices**: Transition to newer models that receive active security updates as the affected devices are no longer supported.
- **Monitor Network Traffic**: Regularly monitor network traffic for any unusual activity that may indicate attempts to exploit these vulnerabilities.
- **Review Security Policies**: Update security policies to reflect the current risks associated with these devices and implement additional network segmentation if necessary.

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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms/