The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
www.cisa.gov/tlp
Information may be distributed without restriction, subject to standard copyright rules.

DATE(S) ISSUED:
08/03/2022

SUBJECT:
Multiple Vulnerabilities in Cisco Small Business RV Series Routers Could Allow for Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Cisco Small Business RV Series Routers, the most severe of which could allow for remote code execution. Cisco Small Business RV Series Routers is a series of routers released by Cisco. Successful exploitation of this vulnerability, could allow a user to execute code in the context of the router.

THREAT INTELLIGENCE:
There are currently no reports of this vulnerability being exploited in the wild.

SYSTEMS AFFECTED:

- RV160 VPN Routers
- RV160W Wireless-AC VPN Routers
- RV260 VPN Routers
- RV260P VPN Routers with PoE
- RV260W Wireless-AC VPN Routers
- 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

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Cisco Small Business RV Series Routers, the most severe of which could allow for remote code execution. Cisco Small Business RV Series Routers is a series of routers released by Cisco. Details of this vulnerability are as follows:

Tactic: *Execution* (TA00041):

Technique: *Native Code* (T1575), *Command and Scripting Interpreter* (T1059):

- CVE-2022-20827 – A vulnerability in the web filter database update feature of Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to perform a command injection and execute commands on the underlying operating system with root privileges.
- CVE-2022-20841 – A vulnerability in the Open Plug and Play (PnP) module of Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to inject and execute arbitrary commands on the underlying operating system.
- CVE-2022-20842 – A vulnerability in the web-based management interface of Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly, resulting in a denial of service (DoS) condition.

Successful exploitation of this vulnerability, could allow a user to execute code in the context of the root user on the underlying operating system.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate patches provided by Cisco to vulnerable systems, immediately after appropriate testing. (**M1051: Update Software**)
    - **Safeguard 7.1: Establish and Maintain a Vulnerability Management Process**: Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
    - **Safeguard 7.4: Perform Automated Application Patch Management:** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.

    - **Safeguard 7.5: Perform Automated Vulnerability Scans of Internal Enterprise Assets:** Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.
- Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring. (**M1050: Exploit Protection)**
    - **Safeguard 10.5: Enable anti-exploitation features on enterprise assets and software, where possible, such as Apple® System Integrity Protection (SIP) and Gatekeeper™.**

REFERENCES:

Cisco:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20827
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20841
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20842