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
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
02/03/2021

SUBJECT:
Multiple Vulnerabilities in Cisco VPN Routers Could Allow for Arbitrary Code Execution.

OVERVIEW:
Multiple vulnerabilities have been discovered in Cisco VPN Routers, the most severe of which could allow for arbitrary code execution as the root user of an affected device. These VPN routers are often used to connect hosts via the router hardware as opposed to individual installations on each device.

Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution in the context of the root user of an affected device. An attacker could then view, change, or delete data and perform other unauthorized actions on the affected device.

THREAT INTELLIGENCE:
There are no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- RV160 VPN Router w/firmware prior to Release 1.0.01.02
- RV160W Wireless-AC VPN Router w/firmware prior to Release 1.0.01.02
- RV260 VPN Router w/firmware prior to Release 1.0.01.02
- RV260P VPN Router with POE w/firmware prior to Release 1.0.01.02
- RV260W Wireless-AC VPN Router w/firmware prior to Release 1.0.01.02

The following products are confirmed to be UNAFFECTED:

- RV340 Dual WAN Gigabit VPN Router
- RV340W Dual WAN Gigabit Wireless-AC VPN Router
- RV345 Dual WAN Gigabit VPN Router
- RV345P Dual WAN Gigabit POE VPN Router

RISK:
Government:

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

Businesses:

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

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Cisco VPN Routers, the most severe of which could allow for arbitrary code execution as the root user of an affected device. The vulnerabilities exist due to improper validation of HTTP requests to the web-based management interfaces of the affected devices. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device.

Details of the CVEs have not been released yet, but their IDs are as follows:

- CVE-2021-1289
- CVE-2021-1290
- CVE-2021-1291
- CVE-2021-1292
- CVE-2021-1293
- CVE-2021-1294
- CVE-2021-1295

Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution in the context of the root user of an affected device. An attacker could then view, change, or delete data and perform other unauthorized actions on the affected device.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate updates provided by Cisco to vulnerable systems immediately after appropriate testing.
- Block external access at the network boundary, unless external parties require service.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Cisco:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1289
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1290
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1291
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1292
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1293
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1294
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1295