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
https://www.cisa.gov/tlp
Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

DATE(S) ISSUED:
04/09/2021

SUBJECT:
Multiple Vulnerabilities in Cisco RV Series Routers Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Cisco RV series small business routers, the most severe of which could allow for arbitrary code execution. The Cisco RV series routers are recommended for connecting your small business' internal network devices to each other. Successful exploitation of the most severe of these vulnerabilities could allow an unauthenticated, remote attacker to execute arbitrary code on the affected systems.

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

SYSTEMS AFFECTED:
- RV160, RV160W, RV260, RV260P, and RV260W prior to 1.0.01.03
- RV340, RV340W, RV345, and RV345P prior to 1.0.03.21

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

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

Home users: N/A

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Cisco RV series small business routers, the most severe of which could allow for arbitrary code execution Details of these vulnerabilities are as follows:

- A vulnerability in the web-based management interface could allow for arbitrary code execution on the affected device due to insufficient user input validation. An attacker could exploit this vulnerability by sending malicious requests to the affected device and executing arbitrary commands on the underlying OS (CVE-2021-1473).

- A vulnerability in the web-based management interface could allow for authentication bypass and uploading of files to directories that should require administrative authentication. This vulnerability occurs due to an improper session management flaw on the affected device. An attacker utilizing specially crafted HTTP requests can upload files to restricted directories (CVE-2021-1472).

Successful exploitation of the most severe of these vulnerabilities could allow an unauthenticated, remote attacker to execute arbitrary code on the affected systems.

RECOMMENDATIONS:
The following actions should be taken:

- Install the update provided by Cisco immediately after appropriate testing.
- Disable the Remote Management for the affected devices
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Cisco:

- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-bypass-inject-Rbhgvfdx

CVE:

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1472
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1473