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:
02/03/2022

SUBJECT:
Multiple Vulnerabilities in Cisco Products Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Cisco Products, the most severe of which could allow for arbitrary code execution. Successful exploitation of the most severe of these vulnerabilities could allow an unauthenticated, remote attacker to execute code on the affected systems. Depending on the privileges associated with the targeted user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users configured to have fewer privileges on the system could be less impacted than those who operate with elevated privileges.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities 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: **Medium**
- Small government: **Medium**

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

Home users: **Low**

TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in Cisco Products where successful exploitation of the most severe could allow for arbitrary code execution. Details of the vulnerabilities are as follows:

- A vulnerability in the SSL VPN module of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. (CVE-2022-20699, CWE-285)
- Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV Series Routers could allow a remote attacker to elevate privileges to *root*. (CVE-2022-20700, CVE-2022-20701, CVE-2022-20702 and CWE-269)
- A vulnerability in the software image verification feature of Cisco Small Business RV Series Routers could allow an unauthenticated, local attacker to install and boot a malicious software image or execute unsigned binaries on an affected device. (CVE-2022-20703 and CWE-434)
- A vulnerability in the software upgrade module of Cisco Small Business RV Series Routers could allow an unauthenticated, remote attacker to view or alter information that is shared between an affected device and specific Cisco servers (cloudsso.cisco.com and api.cisco.com). (CVE-2022-20704 and CWE-552)
- A vulnerability in the session management of the web UI of Cisco Small Business RV Series Routers could allow an unauthenticated, remote attacker to defeat authentication protections and access the web UI. The attacker could obtain partial administrative privileges and perform unauthorized actions. (CVE-2022-20705, CWE-285)
- A vulnerability in the Open Plug and Play (PnP) module of Cisco Small Business RV Series Routers could allow an unauthenticated, remote attacker to inject and execute arbitrary commands on the underlying operating system. (CVE-2022-20706, CWE-77)
- Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an unauthenticated, remote attacker to inject and execute arbitrary commands on the underlying operating system. (CVE-2022-20707, CVE-2022-20708, CVE-2022-20749, CWE-77)
- 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 upload arbitrary files to an affected device. (CVE-2022-20709, CWE-434)
- A vulnerability in the internal interprocess communication of Cisco Small Business RV Series Routers could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition in the login functionality of the web-based management interface. (CVE-2022-20710, CWE-785)
- A vulnerability in the web UI of Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an unauthenticated, remote attacker to overwrite certain files on an affected device. (CVE-2022-20711, CWE-785)
- A vulnerability in the upload module of Cisco Small Business RV Series Routers could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. (CVE-2022-20712, CWE-77)

Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution in the context of the targeted user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new

accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Install the update provided by Cisco immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Cisco:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-mult-vuln-KA9PK6D

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20699
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20700
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20701
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20702
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20703
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20704
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20705
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20706
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20707
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20708
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20709
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20710
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20711
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20712
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20749

CWE:
https://cwe.mitre.org/data/definitions/77.html
https://cwe.mitre.org/data/definitions/269.html
https://cwe.mitre.org/data/definitions/285.html
https://cwe.mitre.org/data/definitions/434.html
https://cwe.mitre.org/data/definitions/552.html
https://cwe.mitre.org/data/definitions/785.html

TLP: WHITE
https://www.cisa.gov/tlp