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:
08/09/2019

SUBJECT:
Multiple Vulnerabilities in Cisco Small Business 220 Series Smart Switches Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Cisco Small Business 220 Series Smart Switches, the most severe of which could allow an unauthenticated, remote attacker to execute arbitrary code with root privileges on a targeted system. Successful exploitation of the most severe of these vulnerabilities could result in a remote attacker obtaining root access to a device running a vulnerable firmware version.

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

SYSTEMS AFFECTED:
- Cisco Small Business 220 Series Smart Switches firmware versions prior to 1.1.4.4

RISK:
Government:
- Large and medium government entities: **High**
- Small government: **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 220 Series Smart Switches, the most severe of which could allow an unauthenticated, remote attacker to execute arbitrary code with root privileges on a targeted system. An attacker could exploit these vulnerabilities by sending malicious requests to the web management interface of an affected device. The vulnerabilities are due to insufficient validation of user-supplied input and improper boundary checks when reading data into an internal buffer. The web management interface is enabled via both HTTP and HTTPS by default. A remote attacker could also perform arbitrary code execution with root privileges by compromising an authenticated user with privilege level 15 on the web management interface. Details of these vulnerabilities are as follows:

- An authentication bypass vulnerability could allow for remote file upload due to incomplete authorization checks in the web management interface (CVE-2019-1912)
- Multiple vulnerabilities could allow for remote code execution due to insufficient validation of user-supplied input and improper boundary checks (CVE-2019-1913)
- A command injection vulnerability could allow for arbitrary code execution by an authenticated attacker due to insufficient validation of user-supplied input (CVE-2019-1914)

Successful exploitation of the most severe of these vulnerabilities could result in a remote attacker obtaining root access to a device running a vulnerable firmware version.

RECOMMENDATIONS:
The following actions should be taken:

- Install the update provided by Cisco immediately after appropriate testing.
- Unless required, limit external network access to affected products.
- 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-20190806-sb220-auth_bypass
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190806-sb220-rce
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190806-sb220-inject

CVE:

- https://nvd.nist.gov/vuln/detail/CVE-2019-1912
- https://nvd.nist.gov/vuln/detail/CVE-2019-1913
- https://nvd.nist.gov/vuln/detail/CVE-2019-1914

Chris Watts
Security Operations Analyst
MS Department of Information Technology Services
601-432-8201 | www.its.ms.gov