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:
01/21/2022

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:
- Cisco RCM for StarOS releases prior to 21.25.4
- Cisco Webex Meetings
- Vulnerable releases of ConfD.
- Cisco Ultra Gateway Platform
- Cisco Enterprise NFV Infrastructure Software (NFVIS)
- Cisco Network Services Orchestrator (NSO)
- Cisco Virtual Topology System (VTS)
- Cisco Carrier Packet Transport1
- Cisco SD-WAN vBond Software
- Cisco SD-WAN vEdge Routers
- Cisco SD-WAN vManage Software
- Cisco SD-WAN vSmart Software
- Cisco IOS XE SD-WAN
- Cisco IOS XR (64-Bit) Software
- Cisco Snort Software releases earlier than Release 2.9.18 and Release 3.1.0.100. Modbus inspection is enabled by default..
- Firepower Threat Defense (FTD) Software - All platforms
- Cybervision Software
- Meraki MX Series Software

- Cisco UTD Software Release
- 1000 Series Integrated Services Routers (ISRs)
- 4000 Series Integrated Services Routers (ISRs)
- Catalyst 8000V Edge Software
- Catalyst 8200 Series Edge Platforms
- Catalyst 8300 Series Edge Platforms
- Catalyst 8500 Series Edge Platforms
- Catalyst 8500L Series Edge Platforms
- Cloud Services Routers 1000V
- Integrated Services Virtual Routers (ISRv)

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:

- Multiple vulnerabilities in Cisco Redundancy Configuration Manager (RCM) for Cisco StarOS Software could allow an unauthenticated, remote attacker to disclose sensitive information or execute arbitrary commands as the root user in the context of the configured container. (CVE-2022-20648, CVE-2022-20649, CWE-200, and CWE-489)
- A vulnerability in the web-based interface of Cisco Webex Meetings could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based interface. (CVE-2022-20654 and CWE-80)
- A vulnerability in the implementation of the CLI on a device that is running ConfD and multiple Cisco products that could allow an authenticated, local attacker to perform a command injection attack. (CVE-2022-20655 and CWE-78)
- A vulnerability in the Modbus preprocessor of the Snort detection engine could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. (CVE-2022-20685 and CWE-190)

Successful exploitation 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-webex-xss-FmbPu2pe
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cli-cmdinj-4MttWZPB
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-confdcli-cmdinj-wybQDSSh
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-dos-9D3hJLuj
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rcm-vuls-7cS3Nuq

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20648
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20649
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20654
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20655
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20685

CWE:
https://cwe.mitre.org/data/definitions/78.html
https://cwe.mitre.org/data/definitions/80.html
https://cwe.mitre.org/data/definitions/190.html
https://cwe.mitre.org/data/definitions/200.html
https://cwe.mitre.org/data/definitions/489.html