Cisco IOS XE WebUI Remote Exploitation | CVE-2023-20198

Overview

A Cisco vulnerability was published on 2023 October 16 under the ID CVE-2023-20198. It describes an active exploitation of a previously unknown vulnerability in the web UI feature of Cisco IOS XE Software allowing a remote, unauthenticated attacker to create an account on an affected system to gain control of the system.

GE Gas Power has identified several of its own products that include the impacted Cisco firmware version listed below. This feature is not used and is disabled by default on GE equipment based on secure by design configurations. If action was taken to enable this feature after GE product delivery, GE strongly recommends disabling this feature using the guidance provided in the "Remediation/Mitigation" section below.

Affected Products and Versions

GE Products with affected firmware (disabled WebUI feature):
NetworkST 3.1

- Cisco 9200L Switch (Root Bridge & Edge)
- Cisco 9300L Switch (Root Bridge & Distribution)

NetworkST 4.0

- Cisco 9200L Switch (XDH – Crossover)
- Cisco 9300L Switch (External)
- Cisco Router 4331

Additional GE supplied products with unaffected firmware version (disabled WebUI feature)

- Cisco Switch 3850
- Cisco Switch 3750
- Cisco Switch 2960x
- Cisco Switch 2960s
- Cisco Switch IE2000
- Cisco Switch IE3300

Vulnerability Details

This vulnerability affects Cisco IOS XE Software if the web UI feature is enabled. The web UI feature is enabled through the `ip http server` or `ip http secure-server` commands within the device configuration.

Vulnerability Details

To check the firmware version of the switch, log into the switch/router and perform the command "show configuration". The configuration will be displayed with the version of the Cisco firmware

applied. In the example below, IOS XE (highlighted) is installed therefore this product has an affected firmware.

```
!------------------------------------------------------------
!  Configuration: GE_9300_Root_(24Port-4Stack)_v01.txt
!  Date: 2020-09-15
!  IOS XE Gibraltar Version: 16.12.4
!------------------------------------------------------------
```

To verify the WebUI service is disabled, continue to view the config for the following text of “ip http server” and “ip http secure-server”. If these commands are listed as below with the “no” command then the system is not affected by the vulnerability as the WebUI service is disabled. GE by secure design disables the WebUI service.

```
!-------------------------------------
! ***** Disable unused services *****
!-------------------------------------

no ip http server
no ip http secure-server
```

Exploitation Status

Cisco is aware of active exploitation of this vulnerability. GE Gas Power Product Security has not yet observed nor received reports of any exploit attempts against Gas Power Customers.
If a customer identifies that they have a GE product from Cisco with WebUI is enabled, they should check for the following indicators of compromise before proceeding with mitigations. If any indicator of compromise is discovered, they should immediately raise an incident with GE PSIRT.

Check the system logs for the presence of any of the following log messages where user could be `cisco_tac_admin`, `cisco_support` or any configured, local user that is unknown to the network administrator:

```
%SYS-5-CONFIG_P: Configured programmatically by process
SEP_webui_wsma_http from console as user on line
```

```
%SEC_LOGIN-5-WEBLOGIN_SUCCESS: Login Success [user: user] [Source:
source_IP_address] at 03:42:13 UTC Wed Oct 11 2023
```

Note: The `%SYS-5-CONFIG_P` message will be present for each instance that a user has accessed the web UI. The indicator to look for is new or unknown usernames present in the message.

Check the system logs for the following message where filename is an unknown filename that does not correlate with an expected file installation action:

```
%WEBUI-6-INSTALL_OPERATION_INFO: User: username, Install Operation: ADD
filename
```

Remediation/Mitigation

GE strongly recommends that customers disable the HTTP Server feature on Cisco network products supplied by GE. To disable the HTTP Server feature, use the "`no ip http server`" and "`no ip http secure-server`" command in global configuration mode. If both the HTTP server and HTTPS server are in use, both commands are required to disable the HTTP Server feature.

The following decision tree can be used to help determine how to triage an environment and deploy protections:

Are you running IOS XE?

- **No.** The system is not vulnerable. No further action is necessary.
- **Yes.** Is `ip http server` or `ip http secure-server` enabled in the configuration?
  - **No.** The vulnerability is not exploitable. No further action is necessary.
  - **Yes.** Disable Web UI services with the "`no ip http server`" and "`no ip http secure-server`" commands within the configuration.

To disable the WebUI services, log into the switch or router configuration. Enter the configuration mode by invoking the "enable" command and entering the password for configuration mode. Enter the following text:

```
SwitchName>enable
SwitchName>(enter enable password)
SwitchName#configuration terminal
SwitchName (config)#no ip http server
SwitchName (config)#no ip http secure-server
SwitchName (config) #exit
#write memory
```

"Write memory" will save the configuration changes and will ensure that the changes are not reverted in the event of a system reload.

Contact Information

Contact your local GE Services representative for assistance or for additional information.
For Product Security issues or incident/vulnerability reporting: www.ge.com/power/cybersecurity

Document History

Version	Release Date	Purpose
1.0	11/6/2023	Initial Release