SecureLogix Security Bulletin

SecureLogix® UTA Appliance: Mitigation for Cisco IOS XE Software Web UI Privilege Escalation Vulnerability

Synopsis

SecureLogix recently learned that Cisco is aware of active exploitation of a previously unknown vulnerability in the web UI feature of Cisco IOS XE Software when exposed to the Internet or to untrusted networks. This vulnerability allows a remote, unauthenticated attacker to create an account on an affected system with privilege level 15 access. The attacker can then use that account to gain control of the affected system.

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.

The SecureLogix UTA Appliance requires the web UI feature to be enabled in order to interoperate with the Cisco API. This document provides an approved mitigation procedure to address this issue.

The Cisco security advisory is available at the following link:

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z

More Information

The UTA Application requires the HTTP service to be enabled in the CUBE in order for the API (WSAPI) to work and communicate properly with the SecureLogix UTA appliance. However, Cisco confirms in their official Advisory that using Access Control Lists (ACLs) is an approved way to restrict access to the HTTP server from untrusted hosts and networks, making the exploit unreachable until Cisco is able to patch this issue in their HTTP and HTTPS implementations.

IMPORTANT: Implementation of **ip http active-session-modules none** cannot be used, since it will break the API functionality.

Mitigation

As part of SecureLogix deployment procedure, we recommend that customers add ACL entries to restrict access by only allowing communication to the UTA Appliance IP addresses. To address this issue and ensure you are following the Cisco recommendation, we advise that

customers confirm they are restricting access to the HTTP Server feature only to the UTA appliances.

Below is an example of the proper ACL implementation for UTA:

```
ip http server
ip http access-class 75

ip access-list standard 75
10 remark SecureLogix_UTA_ACL
10 permit <UTA_IP_Address>
20 deny any
```

Last Update: 10/17/2023

SecureLogix Corporation

13750 San Pedro, Suite 820 • San Antonio, Texas 78232 • (210) 402-9669 • www.securelogix.com

Support (877) SLC-4HELP • EMAIL support@securelogix.com • https://support.securelogix.com