Cisco Network Switch Security Vulnerability

Date: November 13, 2018

Overview:

Communication networks for the Mark*, EX*, and LS* series of products are designed using the Cisco Catalyst series of network switches. The operating systems used in these switches, referred to as the "IOS", is validated and approved for use by GE. Recently important updates to the approved version of the IOS have been made due to issues identified at customer sites and various security vulnerabilities notifications issued by Cisco. Issues identified in the field include loss of communication and loss of redundancy.

Additionally, a cyber vulnerability has been identified by Cisco that impacts the default configuration installed by GE. The configuration setting that was previously enabled as a default in the GE provided switches has the potential to enable an attack which could disrupt communication on the controls network.

The following are listed for reference:

- 3850 - KB0026306
- 2960X - KB0025954
- 3850/2960X/IE2000 - KB0025957

Environment:

Mark*/EX*/LS* Communication Networks including the following devices:

- Cisco IE2000 – 427A8353G0001 – G0008
- Cisco 2960X – 427A8353G0009 – G0024, G0100 – G0107, and G0200
- Cisco 3850 – 427A8353G0108 – G0127

Recommendations:

For projects where switches were ordered prior to July 1, 2018, which have not been commissioned or placed in service, the IOS versions and configuration changes should be applied to all affected switches.

Network switches ordered after July 1, 2018 from the GE approved supplier (WWT), have been configured with the latest updates and are not impacted, and no action is required.

For systems which have already been commissioned, no action is required at this time unless conditions exist which are impacting the operation of the facility or the customer has raised concerns about the Cisco security alerts. For those customers, please contact the Tech Support

team to open a case and to obtain direction on how to properly communicate with the customer and plan an upgrade to the network switch IOS.

Customers who have a SecurityST system and are currently part of the SecurityST CAP program will receive the IOS file and upgrade procedure as part of an upcoming monthly CAP update.

For impacted switches that will be upgraded, the IOS upgrade procedure requires that the devices are rebooted and as such will disrupt communications, on edge switches this will disrupt all the devices connected, on root switches this will disrupt the entire network. It is highly recommended that any modifications to the IOS are completed during a site outage.

Please, contact your local GE Service Representative to obtain the detailed, step by step procedures for the upgrade of the Cisco IOS. Upgrades should only be attempted by qualified personnel who have been trained in the operation and maintenance of the Cisco IOS.

*Trademark of General Electric Company

https://gepowerpac.service-now.com/kb_view.do?sysparm_article=KB0026307

GE Power Product Security Incident Response Team (PSIRT)

GE is committed to helping ensure the security of its customer base. To report product security issues and to request security support, contact GE Power PSIRT at www.ge.com/power/cybersecurity or GEPowerCVD@ge.com.