Cisco® IOS® Update: 2960X Series

Date: May 23, 2018

Overview:

Failure to communicate with the management interface of the device using the Secure Socket Shell (SSH) protocol, loss of communication on a port, and potential inability to replace a switch in a stacked pair.

Environment:

All Cisco 2960X switches using IOS 15.0.2a EX5 or earlier

Recommendations:

Affected sites need to update cisco switch IOS to version 15.2(5)E2 at the earliest convenience.

Cisco IOS is provided directly by Cisco through a services agreement with the product supplier on supported hardware.

Firmware can be directly downloaded from Cisco website

https://www.cisco.com/c/en/us/products/index.html

Cause:

Memory leak on the 2960X switch that could ultimately result in failure to communicate with the management interface of the device using the Secure Socket Shell (SSH) protocol, loss of communication on a port, and potential inability to replace a switch in a stacked pair.

https://gepowerpac.service-now.com/kb_view.do?sysparm_article=KB0025954

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.