CISCO Catalyst 3850x switches (IOS) vulnerabilities

Date: November 6, 2017

Overview:

Multiple CISCO Internetwork Operating System (IOS) vulnerabilities have been corrected via a CISCO software update. If left uncorrected, an authenticated, remote attacker could remotely execute code and obtain full-control of the affected system or cause the affected system to reload.

Environment:

All new units shipped from GE prior to September 2017 with CISCO Catalyst 3850x switches running IOS versions below 3.7.5E. Units shipped after September 2017 are loaded with CISCO IOS version 3.7.5E (as of October 2017).

Background:

The Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a standardized framework and a common language for monitoring and managing devices in a network. It defines a message format for communication between SNMP managers and agents. The SNMP subsystem of CISCO IOS and IOS XE software contains multiple vulnerabilities. An attacker could exploit these vulnerabilities by sending a crafted SNMP packet to an affected system.

The vulnerabilities are due to a buffer overflow condition in the SNMP subsystem of the affected CISCO software. The vulnerabilities affect all versions of SNMP - versions 1, 2c, and 3. To exploit these vulnerabilities via SNMP version 2c or earlier, the attacker must know the SNMP read-only community string for the affected system. To exploit these vulnerabilities via SNMP version 3, the attacker must have user credentials for the affected system. A successful exploit could allow the attacker to execute arbitrary code and obtain full control of the affected system or cause the affected system to reload.

Updating to CISCO IOS version 3.7.5E or later and updating switch configuration per CISCO's recommendations in the CISCO Security Advisory link below will mitigate these vulnerabilities. This link also describes how to determine which CISCO IOS software release is currently running on a device. Details of required modifications to the configuration script are described in the Workarounds section of the advisory. Contact GE if the link is inaccessible.

CISCO Security Advisory

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170629-snmp

To date, there have been no known infections on GE turbine control/monitoring networks.

Advisory:

Due to the wide variety and continuous development of malware and other cyber threats, GE generally recommends adhering to all reasonable security practices.

- Maintain a separation of ICS and corporate networks. Where impossible, implement an access control list that logs and prevents ICS networks and systems from establishing connections with indiscriminate and unknown internet hosts and devices.
- Disable unnecessary removable media ports and devices (USB, CD/DVD, etc.) and disconnect unnecessary network shares.
- Review current site security policy. Specifically address removable media, including USB memory devices, in the corporate security policy. Develop, document, and test a strong incident response plan.
- Ensure antivirus security software updates and virus protections are current.
- Evaluate the vulnerability of the control systems against safety and availability requirements.
- Monitor for new updates continually, including Microsoft Windows patches.
- Regularly patch software as updates become available.

Due to the variation in customer networks, GE cannot validate all firmware or software patch updates released by manufacturers. The following is recommended if users decide to apply patches.

1. Take an image backup of the device to be updated (HMI, historian, etc.)
2. Update the antivirus definitions/software.
3. Run and install the applicable software update/patch. In rare instances, updates/patches may impact the device's function. As such, new updates should be tested within a testbed platform before installing into a production environment. If a testbed is not feasible, apply update to only one or two devices before being propagated to the entire plant.

Please contact your local GE representative for additional information or assistance.
https://gepowerpac.service-now.com/kb_view.do?sysparm_article=KB0024911

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.