Security Notification – Magelis HMI - Version 2

7/14/2017

Overview

Schneider Electric is aware of vulnerabilities identified by researcher Eran Goldstein on Magelis Human Machine Interface (HMI) products, and is providing this document to advise users on mitigations to help minimize exposure.

Vulnerability Overview

The use cases identified demonstrate the ability to generate a freeze conditions on the HMI, that can lead to a denial of service due to incomplete error management of HTTP requests in the Web Gate Server. While under attack via a malicious HTTP request, the HMI may be rendered unable to manage communications due to high resource consumption. This can lead to a loss of communications with devices such as Programmable Logic Controllers (PLCs).

Exploitation of these vulnerabilities requires the Web Gate Server to be activated. By default, this function is disabled.

The following CVSS scores have been assessed for the identified vulnerabilities:

Uncontrolled Resource Consumption (1)
An attacker can open multiple connections to a targeted web server and keep connections open preventing new connections from being made, rendering the web server unavailable during an attack.

- CVSS Score = 5.3
- CVSS:3.0 vector string (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)

Uncontrolled Resource Consumption (2)
This issue exists only for Runtime versions prior to 6.2SP2. Newer versions are not impacted.

An attacker may be able to disrupt a targeted web server, resulting in a denial of service, requiring the affected device to be rebooted in order to regain operation.

- CVSS Score = 7.5
- CVSS:3.0 vector string (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Schneider Electric wishes to thank Eran Goldstein for his research and collaboration on assessing these issues, and commends his responsible disclosure practices.

Product(s) Affected

The following Schneider Electric Magelis HMI products are affected:

- Magelis GTO Advanced Optimum panels
- Magelis GTU Universal panel
- Magelis STO5xx & STU Small panels & SCU
- Magelis XBT GH Advanced Hand-held Panel
- Magelis XBT GK Advanced Touchscreen Panels with Keyboard
- Magelis XBT GT Advanced Touchscreen Panels
- Magelis XBT GTW Advanced Open Touchscreen Panels (Windows XPe)

Mitigation

To minimize potential exposure, users of all affected versions are advised to:

Ensure the latest software/firmware is installed

- Users with products having Runtime versions prior to 6.2SP2 are advised to upgrade to the latest available version, available from www.schneider-electirc.com. Current versions of the Runtime do not require a reboot for the HMI to recover from attack.

General Security Best Practices

- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet
- Minimize potential attack surface by leaving the Web Gate Server set to its default disabled state if it is not needed

Additional Mitigations (Local Area Network)

- Place control system networks and devices behind firewalls (such as the ConneXium Tofino Firewalls), and isolate them from the business network
- Limit traffic on the local network with managed switches (such as ConneXium managed switches)
- Where possible, avoid Wi-Fi capabilities
- When Wi-Fi is essential, use only secure communications (such as WPA2 encryption)
- Do not grant access to unknown computers

Additional Mitigations (Wide Area Network)

- When remote access is essential, use secure methods such as Virtual Private Networks (VPNs), and ensure the remote access solution(s), as well as the remote computer(s) are kept up-to-date with the latest security patches.

Upgrade Options

In addition, current owners of the following affected products can upgrade Vijeo Designer v2.4.2 to a new software offer with new Runtime for their units here: http://www.schneider-electric.com/en/download/document/Vijeo_XD_2016_SP2_v2.4.2/

- Magelis GTO Advanced Optimum panels
- Magelis GTU Universal panel

For More Information

This document is intended to help provide an overview of the identified vulnerabilities and recommended actions to help minimize exposure. To obtain full details on these issues, and assistance on protecting your installation, please contact your local Schneider Electric representative.

For further information on vulnerabilities in Schneider Electric products, please visit the Schneider Electric cybersecurity web page at http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

References

Connexium Tofino Firewall:

http://www.schneider-electric.fr/fr/download/document/NHA1573401/

Connexium Managed Switch:

http://www.schneider-electric.com/ww/en/download/document/31007122K01000

About Schneider Electric: Schneider Electric is the global specialist in energy management and automation. With revenues of €27 billion in FY2015, our 160,000 employees serve customers in over 100 countries, helping them to manage their energy and processes in ways that are safe, reliable, efficient and sustainable. From the simplest of switches to complex operational systems, our technology, software and services improve the way our customers manage and automate their operations. Our connected technologies will reshape industries, transform cities and enrich lives. At Schneider Electric, we call this **Life Is On**.

www.schneider-electric.com

Revision Control:

Version 1 *21 Nov 2016*	Original Release
Version 2 *14 July 2017*	Page 2 - Updated **Mitigation** section with link to updated software

Product Security Office

Digitally signed by Product Security Office
DN: cn=Product Security Office, o=Schneider Electric, ou=Global Technology, email=cybersecurity@schneider-electric.com, c=US
Date: 2017.07.14 13:00:59 -04'00'