Security Notification – EcoStruxure Substation Operation User Interface

7-Dec-2017

Overview

Schneider Electric has become aware of vulnerabilities in the MySQL Server version 5.5.56 product. This product is used in EcoStruxure Substation Operation User Interface (Formerly EcoSUI)

Vulnerability Overview

MySQL server is used in EcoStruxure Substation Operation User Interface (formerly EcoSUI) as an operational database.

The CVE ID list of vulnerabilities identified are below:

- CVE-2017-3635
- CVE-2017-3636
- CVE-2017-3641
- CVE-2017-3651
- CVE-2017-3652

Product(s) Affected

The product(s) affected:

- MySQL Server version 5.5.56 and earlier impacting EcoStruxure Substation Operation User Interface (formerly EcoSUI) version 2.1.17279 and earlier.

Vulnerability Details

These vulnerabilities can allow a privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks can result:

- In unauthorized update, insert or delete access to some of MySQL Server accessible data.

- Cause a hang or frequently repeatable crash (complete DOS) of MySQL Connectors.

Mitigation

Schneider Electric **recommends installing an updated version of** EcoStruxure Substation Operation User Interface (formerly EcoSUI) integrating a new version of MYSQL starting from EcoSUI V2.1.17285.

Mitigation

Given that vulnerabilities take effect once an attacker gains network access and or local access to the server, mitigation actions can be taken to reduce risk:

- Secure Network Access (Switch Configuration, Physical Security).
- Put in place Network Intrusion Detection System to monitor network activities.
- Apply strong security policies on servers to limit attack surface (Hardening measure, Password length, Complexity, Low privilege definition…)

For Secure Network Access is recommended to define strong hardening rules in Network Devices:

- Disable Unused Services and port (Secure management protocol, Physical port, VLAN)
- IP filtering configuration to limit access
- Track changes in Network (MAC changes, IPs.) to alert and monitor network activities
- Log Monitoring (Audit) alert and monitor activities

Contact your local support for more information:

https://www.schneider-electric.com/b2b/en/support/

For More Information

This document is intended to help provide an overview of the identified vulnerability and actions required to mitigate it. To obtain full details on the issues and assistance on how to protect your installation, please contact your local Schneider Electric representative. These organizations will be fully aware of the situation and can support you through the process.

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

About Schneider Electric

Schneider Electric is the global specialist in energy management and automation. With revenues of ~€25 billion in FY2016, our 160,000+ employees serve customers in over 100 countries, helping them to manage their energy and process 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 reshape industries, transform cities and enrich lives. At Schneider Electric, we call this **Life Is On**.

www.schneider-electric.com

Revision Control:

Version 1 *07 December 2017*	Original Release

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: 2017.12.07 19:17:56 -05'00'