Security Notification - ClearSCADA

21-Sep-2017

Overview

Schneider Electric has become aware of a vulnerability in the ClearSCADA product line.

Vulnerability Overview

The vulnerability identified is as follows:

- ClearSCADA versions released prior to August 2017 are susceptible to a memory allocation vulnerability, whereby malformed requests can be sent to ClearSCADA client applications to cause unexpected behavior. Client applications affected include ViewX and the Server Icon.

Product(s) Affected

The product(s) or product lines affected include:

- All supported versions including:
  - ClearSCADA 2017 — Released March 2017
  - ClearSCADA 2015 R2 — Released February 2016
  - ClearSCADA 2015 R1.1 — Released January 2017
  - ClearSCADA 2015 R1 — Released June 2015
- All prior versions

Vulnerability Details

A malicious actor with network access to the ClearSCADA client applications (including those running on the server e.g. Server Icon) can build and send specific sequences of commands and data packets to the ClearSCADA client that can cause unexpected behavior in the ViewX and Server Icon applications. These applications receive data from the server to update their displays.

There is no evidence that this vulnerability has been exploited in a production environment.

This vulnerability only affects ClearSCADA clients. It does not directly affect the ClearSCADA server or drivers.

Overall CVSS Score: 5.3 (Medium)

(CVSS V3 Vector): 3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L.

CVE ID: CVE-2017-9962 **https://cve.mitre.org/cgi-bin/cvename.cgi?name=2017-9962**

Mitigation

Schneider Electric advises all ClearSCADA users to take steps to secure physical and network interfaces to the ClearSCADA system, and to log out of Windows on the Server machine when unattended. Schneider Electric advises customers to include the following measures in their SCADA strategies:

- Deploy suitably configured firewalls between network segments to limit access to ports and protocols appropriately.
- Deploy VPN technology with secure authentication on any externally accessible networks.
- Configure and audit user security to reduce the risk of a denial of service. For critical accounts use ClearSCADA security policy configuration to disable invalid logon count and delayed lockout time and to use logon throttling.
- Log out of Windows on the Server Machine so the ServerIcon.exe process and ViewX application are not left running when not in use.

Schneider Electric has recently corrected this vulnerability which has been made available in the following Monthly Update releases, including any future Monthly Update releases (with a higher 4-digit build number) of each version:

1. ClearSCADA 2017 - August 2017 Update (build 78.6439) Available 28 Aug 17.
2. ClearSCADA 2015 R2 - August 2017 Update (build 77.6438) Available 28 Aug 17.
3. ClearSCADA 2015 R1.1 - August 2017 Update (build 76.6428) Available 28 Aug 17.

Users of ClearSCADA 2014 R1 and prior versions are recommended to upgrade to the latest ClearSCADA 2017 Update to benefit from these security improvements.

If you wish to upgrade, the latest Monthly Update releases of each of the above versions are available for direct download from the Schneider Electric website:

http://resourcecenter.controlmicrosystems.com/display/CS/ClearSCADA+Downloads

To update your license (not required when upgrading to a Monthly Update, Service Pack, or hotfix of the same version), customers are required to complete and submit an online form available here:

http://resourcecenter.controlmicrosystems.com/display/CS/ClearSCADA+Update+Request+Form

Acknowledgements

Schneider Electric wishes to thank Artem Baranov of Critical Infrastructure Defense Team, Kaspersky Lab for identifying and Vladimir Dashchenko of Critical Infrastructure Defense Team, Kaspersky Lab for all their efforts related to identification and coordination of this vulnerability, and working with Schneider Electric during the disclosure process.

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 *21 September 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: 2017.09.20 14:41:52 -04'00'