# Security Notification- SCADA Expert ClearSCADA

1-Mar-2017

## Overview

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

## Vulnerability Overview

The vulnerability is identified as follows:

- SCADA Expert ClearSCADA versions released prior to December 2016 are susceptible to a communications vulnerability, whereby malformed requests can be sent to the ClearSCADA server to cause termination of the ClearSCADA DBServer process.

## Product(s) Affected

The product(s) or product lines affected include:

- All supported versions including:
  - ClearSCADA 2014 R1 (build 75.5210) Released April 2014
  - ClearSCADA 2014 R1.1 (build 75.5387) Released October 2014
  - ClearSCADA 2015 R1 (build 76.5648) Released June 2015
  - ClearSCADA 2015 R2 (build 77.5882) Released February 2016
- All prior versions

## Vulnerability Details

A malicious actor with network access to the ClearSCADA server can build and send specific sequences of commands and data packets to the ClearSCADA server that can cause the ClearSCADA server process and ClearSCADA communications driver processes to terminate.

- There is no evidence that this vulnerability has been exploited in a production environment.
- CVSS v3 Base Score of 7.5 has been assigned
- The CVSS vector string is 3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H.

## Mitigation

Schneider Electric advises all ClearSCADA users to take steps to secure physical and network interfaces to the ClearSCADA system. 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.

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

1. ClearSCADA 2014 R1.1 hotfix build 75.6239 — Available 31 Jan 17.
2. ClearSCADA 2015 R1.1 Service Pack (build 76.6191) — Available 13 Dec 16.
3. ClearSCADA 2015 R2 hotfix build 77.6181 — Available 04 Dec 16.

The above hotfix versions of ClearSCADA have been published to expedite their availability prior to the official release of a Service Pack for those versions which will be made available in due course.

Users of ClearSCADA 2013 R2 and prior versions are recommended to upgrade to the latest ClearSCADA 2015 R2 hotfix to benefit from these security improvements.

If you wish to upgrade please contact your local Schneider Electric office for latest ClearSCADA release, alternatively the latest Service Pack and hotfix releases of each of the above versions are available for direct download from the Schneider Electric website:

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

To update your license (not required when upgrading to a 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/StruxureWare+SCADA+Expert+ClearSCADA+Update+Request+Form

Schneider Electric wishes to thank Sergey Temnikov of Critical Infrastructure Defense Team, Kaspersky Lab for identifying and Vladimir Dashchenko of Critical Infrastructure Defense Team, Kaspersky Lab for reporting of the 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.schneiderelectric.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 €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.

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: 2017.02.23 09:05:03 -05'00'