Important security notification – Schneider-Electric

SCADA Expert ClearSCADA DNP3 Driver Fuzzing Vulnerability

December 5, 2013

Schneider Electric® has become aware of a vulnerability involving the StruxureWare SCADA Expert ClearSCADA software.

The vulnerability identified:

- SCADA Expert ClearSCADA versions released prior to November 2013 are vulnerable to specific DNP3 fuzzing attacks, which could cause excessive logging and in extreme cases result in a denial of service.
- There is no evidence that this vulnerability has been exploited in a production environment.

Schneider Electric takes these vulnerabilities very seriously and we have devoted resources to immediately investigate and address these issues. We believe it is critical to consider the whole picture, including safety, security and reliability. Any patches/solutions/mitigations we release will be carefully tested to ensure that they can be deployed in a manner that is both safe and secure.

Details on Products Affected

The following supported software versions are affected by the SCADA Expert ClearSCADA DNP3 Driver Fuzzing vulnerability:

- ClearSCADA 2010 R2 (build 71.4165) — Released May 2011
- ClearSCADA 2010 R2.1 (build 71.4325) — Released November 2011
- ClearSCADA 2010 R3 (build 72.4560) — Released June 2012
- ClearSCADA 2010 R3.1 (build 72.4644) — Released September 2012
- SCADA Expert ClearSCADA 2013 R1 (build 73.4729) — Released December 2012
- SCADA Expert ClearSCADA 2013 R1.1 (build 73.4832) — Released March 2013
- SCADA Expert ClearSCADA 2013 R1.1a (build 73.4903) — Released June 2013
- SCADA Expert ClearSCADA 2013 R1.2 (build 73.4955) — Released July 2013

Details on workarounds or planned fix dates for above described Vulnerability

Schneider Electric has fixed this issue in the latest released software version of SCADA Expert ClearSCADA 2013 R2.

Please contact your local Schneider Electric office for latest software version for ClearSCADA; alternatively this new version is available for direct download from the Schneider Electric website. To upgrade, customers are required to complete and submit an online form available here:

http://telemetry.schneider-electric.com/id2/form/CMIform.html

General instructions on how to upgrade your ClearSCADA license are available here:

http://resourcecenter.controlmicrosystems.com/display/CS/Updating+Your+ClearSCADA+License

Detailed instructions on how to upgrade a ClearSCADA installation are available here:

http://resourcecenter.controlmicrosystems.com/display/CS/SCADA+Expert+ClearSCADA+2013+R2+Upgrade+Strategy

General Recommendations

Schneider Electric has been designing industrial automation products for many years; Schneider Electric follows, and recommends to its customers, industry best practices in the development and implementation of control systems. This recommendation includes a Defense in Depth approach to secure an Industrial Control System.

Download our cybersecurity whitepaper from www.schneider-electic.com. See Support > Cybersecurity

Schneider Electric advises all ClearSCADA users to take steps to secure the interfaces to the ClearSCADA system. The following guidelines should be taken as a starting point only in establishing an appropriate level of system security:

- Monitor DNP3 traffic and system Event Journal to detect excessive amounts of traffic/logging which may be representative of a fuzzing attack.
- Upgrade the ClearSCADA server to SCADA Expert ClearSCADA 2013 R2 or newer, or Service Packs released later than November 2013.

Acknowledgements

Schneider Electric wishes to thank Adam Crain of Automatak and independent researcher Chris Sistrunk for reporting of the vulnerability and working with Schneider Electric during the disclosure process.

Support CVSS Scoring

CVSS scores are a standard way of ranking vulnerabilities and are provided for reference based on a typical control system they should be adapted by individual users as required.

For the CVSS cognoscenti, the vector is (AV:N/AC:M/Au:N/C:N/I:N/A:P)

CVSS Base Score: 4.3