Security Notification – VAMPSET

11 May 2017

Overview

Schneider Electric has become aware of a vulnerability in the VAMPSET setting and configuration software product. This software is used to configure and maintain multiple protection relays and arc flash protection units.

Vulnerability Overview

The vulnerability is identified as follows:

- VAMPSET is susceptible to a memory corruption vulnerability when a corrupted vf2 file is used. This vulnerability causes the software to halt or not start when trying to open the corrupted file. As Windows operating system remains operational and VAMPSET responds, it is able to be shut down through its normal closing protocol.

Product(s) Affected

The product(s) affected:

- VAMPSET, all versions prior to v2.2.189 version

Vulnerability Details

This vulnerability occurs when fill settings are intentionally malformed and is opened in a stand-alone state, without connection to a protection relay. This attack is not considered to be remotely exploitable. This vulnerability has no effect on the operation of the protection relay to which VAMPSET is connected.

Overall CVSS Score: 5.5 (Medium)

CVSS: 3.0/AV:L/AC:M/Au:S/C:P/I:P/A:C

CVE ID: CVE-2017-7967: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-7967

Mitigation

The VAMPSET tool has been updated in order to recognize malformed setting files.

VAMPSET file response after corrective action:

- program remains operational and
- reports to the user: “Cannot open file”

A firmware with the fix for this vulnerability is available for download:

http://www.schneider-electric.com/en/download/document/VAMPSET_v2.2.191/

Acknowledgements

Schneider Electric would like to thank Kushal Arvind Shah from Fortinet's Fortiguard Labs for all their efforts related to identification and coordination of this vulnerability.

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

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: 2017.05.11 13:27:30 -04'00'