Important Security Notification

VAMPSET Software

March 25, 2015

Overview

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

Vulnerability Overview

The vulnerability in VAMPSET is caused by opening malformed VAMPSET disturbance recorder files. VAMPSET becomes halted when trying to open a corrupted file. Even though Windows operating system remain operational, VAMPSET does not respond anymore until the corresponding process is terminated. This is caused by a buffer overflow which could result in remote code execution.

Product(s) Affected

The product affected includes:

- VAMPSET software, V2.2.145 and all previous versions

Vulnerability Details

- Malformed or corrupted disturbance recording files causes VAMPSET to crash, when opened in stand-alone state, without connection to a protection relay. VAMPSET is vulnerable to a Stack-based and Heap-based buffer overflow attack, which can be exploited by attackers to execute arbitrary code, by providing a malicious CFG or DAT file with specific parameters. This vulnerability has no effect on the Windows Operating System
    - CVSS score = 6.6 (AV:L/AC:M/Au:N/C:P/I:C/A:C)

Mitigation

VAMPSET software was developed with the expressed intention of providing an easy means for maintenance personnel to modify or manage the configuration parameters of multiple protection relays. This software is designed to be used in close proximity to the protective relay. It is always a real possibility that an attacker provides or modifies the configuration file and leaves VAMPSET tool to handle it. In case the file is intentionally corrupted the setting tool fails to open it and could stop VAMPSET setting tool program.

The normal protocol when disturbance recording files are used is as follows:

a) User reads the disturbance file in the VAMPSET with direct connection to a device or

b) Having stored the file in hard disk user opens the file directly from computer disk

The reported attack test was stopped at the file opening stage (a) after the file was intentionally made malformed.

To protect the computer and configuration files from unauthorized escalation of privileges through manipulation, Schneider Electric recommends users employ best IT practices to secure their computers and relay's configuration files, use of User Access Control (UAC) can further improve the security of the computer. Additionally, to minimize the risk of attack, users who are not directly using this software on a regular basis are strongly encouraged to delete this application from their computer to reduce the likelihood of attack and to store relay's configuration files in the client's protected location.

The VAMPSET tool has been updated as described below in order to recognize malformed disturbance recorder file.

Disturbance recorder files recognition:

- The length of the text string in the Comtrade file is checked in order to recognize them being acceptable for the tool. This means that the station name and device identification must be proper in length.

In case above conditions are not met the software

- block opening such file,
- remain operational and
- reports to the user that the file is not complete or contains wrong data.

The above stated release is made public and released for distribution on 20 March, 2015. Link to the VAMPSET setting tool v.2.2.168 or newer is as follows:

http://www.schneider-electric.com/products/ww/en/2300-ied-user-software/2320-vamp-user-software/62050-vamp-software/

Schneider Electric would like to thank Mr. Ricardo Narvaja from Core Exploit Writing Team for all his efforts related to identification of this vulnerability. The publication of this advisory was coordinated by Mr. Joaquín Rodríguez Varela from Core Advisories Team

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

As a global specialist in energy management with operations in more than 100 countries, Schneider Electric offers integrated solutions across multiple market segments, including leadership positions in Utilities & Infrastructures, Industries & Machine Manufacturers, Non-residential Buildings, Data Centers & Networks and in Residential.
www.schneider-electric.com