Important Security Notification

VAMPSET Software

4-Sep-2014

Overview

Schneider Electric was notified and is responding to vulnerability in the VAMPSET software product. This software is used to configure and maintain multiple protection relays and arc monitoring units.

Vulnerability Overview

The vulnerability in VAMPSET is caused by opening corrupted VAMPSET setting files or disturbance recording files. This vulnerability consists in VAMPSET become halted when trying to open a corrupted file. Even though Windows operating system remain operational, VAMPSET did not respond anymore until the corresponding process was terminated.

Product(s) Affected

The product affected includes:

- VAMPSET, v2.2.136 and all previous versions.

Vulnerability Details

- Corrupted configuration or disturbance recording files make VAMPSET crash.
- The setting tool becomes halted but Windows operating system remains operational.
- This phenomenon happens when configuration or disturbance configuration file is corrupted and is opened in stand-alone state, without connection to a protection relay.
- The configuration file must be opened by VAMPSET first before a possible download in the relay is made. As the opening of the inadequate setting file fails there is not possibility to have this file downloaded to the protection relay. On the other hand each setting parameter is checked and verified before storing it in the relay’s database.
- This attack is not considered to be remotely exploitable.

Common Vulnerability Scoring System, CVSS base vector indicated **AV:L/AC:M/Au:S/C:P/I:P/A:P** giving a score of 4,1 which means that the case severity level is **Medium / Moderate.**

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 the 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 setting protection relays is to

a) open the setting file
b) download the file in the protection relay
c) validate the downloaded parameters from the HMI and
d) finally make commissioning / verification of the relay's performance. The reported attack test was stopped at the file opening stage (a).

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 improper configuration or disturbance recorder file.

Setting files recognition:

- the file row length is monitored
- file identification parameters must be found in a right place within the source data

Disturbance recorder files recognition:

- character check added, the file may contain only pre-determined characters
- length of the file is checked
- sampling row numbering is made more extensive

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 update was released for distribution on 21 August, 2014. Link to the VAMPSET setting tool v.2.2.145 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 recommends to all customers and users to install and use VAMPSET v.2.2.145 or newer.

Acknowledgement

Schneider Electric would like to thank Mr. Aivar Liimets from Martem AS, Estonia for all his efforts related to identification 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