GE Multilin SR Protective Relays Passcode Vulnerability

Anastasis Keliris
Tandon School of Engineering
New York University
New York, USA
Email: anastasis.keliris@nyu.edu

Charalambos Konstantinou
Tandon School of Engineering
New York University
New York, USA
Email: ckonstantinou@nyu.edu

Michail Maniatakos
New York University Abu Dhabi
Abu Dhabi, UAE
Email: michail.maniatakos@nyu.edu

***Abstract*—This white paper discusses the CVE-2017-7905 vulnerability discovered in the authentication mechanism of the General Electric Multilin SR power system protection and control products. The vulnerability has been disclosed to General Electric and a series of firmware upgrades for the affected devices has been released. The reported vulnerability falls under CWE-261, Weak Cryptography for Passwords, and has been assigned a CVSS v3 base score of 8.1.**

***Keywords*—Electric power systems, GE Multilin passcode vulnerability, ICSA-17-117-01A, CVE-2017-7905.**

I. Introduction

Electricity has a significant role in our everyday lives and its uninterrupted supply is considered a certainty. Electric power systems are utilized for supplying electric power and are comprised of networked components responsible for generating and transferring electricity to end consumers. From production to consumption, four stages are employed, namely generation, transmission, distribution, and utilization. In the generation stage electricity is produced, typically by gas or steam driven turbines. It is then stepped up to high voltages and travels across large distances in the transmission stage. At locations near power loads it is stepped down to lower voltage levels and enters the distribution stage, where end consumers are connected to distribution substations. Finally, it is utilized by these end consumers, which can be categorized as residential, commercial, or industrial.

The safe and reliable operation of power systems is ensured through the use of protection and control equipment. This equipment monitors voltage and current levels for faults. In the event a fault is detected, protective devices try to isolate it from the rest of the network. In general, protective *relays* sense electrical signals and if they detect a fault they send a tripping signal to circuit breakers. Clearing faults must be done in the shortest possible time to prevent damage to equipment and minimize the possibility of subsequent trips that can destabilize the power system. There are several types of relays used throughout the different stages of a power system: generator protection relays for the generation stage, transformer protection relays for the transmission stage, feeder protection relays for the distribution stage, and motor protection relays in the customer side.

Power grids across the world are undergoing modernization, towards increased efficiency and controllability. This modernization is achieved through the use of microprocessor-based "smart" devices with remote communication capabilities, replacing the electromechanical devices used in the past. Smarter protection and control devices are widely desired, as these devices play a vital role in the reliable and efficient operation of power systems through enhanced visibility, enabling wide area monitoring systems. At the same time, the digitization and increased importance of Information Technology (IT) in power system devices, expand the threat landscape and enable cyberattacks.

This white paper discusses a vulnerability discovered in the authentication mechanism of several relays of the General Electric (GE) Multilin protection and control family of products. The vulnerability allows remote or local attackers to obtain weakly encrypted user passwords, which could then be reversed allowing unauthorized access. Section II provides information regarding the vulnerability. Section III lists affected devices and Section IV discusses mitigation strategies. The paper concludes in Section V.

II. Passcode authentication

When configuring a relay, setpoints are settings that define its specific operational details. For example, to instruct the relay to send a trip command to the circuit breaker whenever the voltage reaches a value that is 80% above the nominal voltage value of the monitored power line, a corresponding setpoint must be configured in the relays settings. Several GE Multilin products require authenticated access for enabling modification of setpoints using a passcode. Knowledge of the passcode enables reconfiguration of all the device setpoints (e.g. overvoltage/overcurrent pickups), including the passcode itself, since the passcode is treated as a setpoint.

The default passcode is `0`, which is a special value that allows reading and writing all setpoints without entering the passcode. When a non-default passcode is set, the device requires the user to input the passcode before allowing any modification of the setpoints. The device then encrypts the user-provided passcode and checks it against the saved encrypted passcode. Passcodes consist of eight numerical digits, each of which can take a value from `0` to `9`. Encrypted passcodes consist of eight characters, where each character can assume a value from `A` to `K`.

The main vulnerability lies in the fact that the value of the encrypted passcode can be read by an unprivileged user:

TABLE I. AFFECTED PRODUCTS

Model	Firmware versions
750 Feeder protection relay	< version 7.47
760 Feeder protection relay	< version 7.47
469 Motor protection relay	< version 5.23
489 Generator protection relay	< version 4.06
745 Transformer protection relay	< version 5.23
369 Motor protection relay	< version 3.63

For a *local* user, it is possible to navigate using the buttons through the available options in the device menu and display the encrypted passcode on the front panel LCD display.

In the case of a *remote* user connecting to the device using Modbus TCP, the encrypted passcode can be read by issuing Modbus read requests. As the Modbus protocol does not incorporate any authentication mechanisms, this information is available to anyone on the same network with the device.

Exacerbating the vulnerability, the passcode is encrypted with a homebrewed encryption algorithm. Thus, with access to encrypted passcodes, we collected a selection of passcodes and their respective encrypted passcodes and launched a Chosen Plaintext Attack (CPA) against the employed encryption algorithm, leveraging manual cryptanalysis techniques. We successfully reverse engineered the inner workings of the algorithm, enabling us to decrypt any arbitrary encrypted passcode and obtain its corresponding plaintext passcode. The ability of decrypting encrypted passcodes combined with the ability of extracting them either locally or remotely allows arbitrary modifications to setpoints, and hence full access to the device functionality. Considering that passcodes themselves are treated as a setpoint, it is possible for an adversary to read the encrypted passcode, decrypt it, and subsequently change the passcode effectively locking the legitimate users of the device out.

Due to the sensitive nature of the target domain, we do not disclose the actual algorithm employed by the affected devices. Instead, we discuss its flaws, which allow manual cryptanalysis:

- Not Using a Random IV with CBC Mode: The homebrewed algorithm uses a fixed IV for encrypting the passcode, making cryptanalysis easier (CWE-329).
- Linearity: The transformations employed by the homebrewed algorithm are linear, enabling known plaintext attacks.

The disclosed vulnerability has been assigned a CVSS v3 base score of 8.1. The CVSS vector string is (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).

III. AFFECTED DEVICES

The vulnerability allowing access to the encrypted passcode and employment of a weak encryption algorithm affects a number of GE Multilin models. The initial ICS-CERT advisory regarding this vulnerability listed six models from the SR family of products to be affected [1]. These products, along with the affected firmware versions are listed in Table I.

IV. MITIGATION STRATEGIES

To mitigate the vulnerability, GE issued firmware updates for the affected products. The firmware updates remove the ability to read encrypted passcodes from both the front panel (for local users) and through Modbus (for remote users). Without the ability to extract the encrypted passcode, an attacker cannot gain unauthorized write access to setpoints and take over a device.

In addition, general Industrial Control Systems (ICS) cyber security best practices and Defense-in-Depth strategies should be followed [2]. For example, physical access to ICS devices should by controlled and passwords should not be reused. Network activity should be monitored. Furthermore, control devices should be placed behind firewalls in a separate control system network, that does not share connections with the business network or the public internet.

V. CONCLUSION

This white paper discussed a vulnerability in the authentication mechanism employed in several GE Multilin protection and control products. The vulnerability allows unauthenticated local and remote access to encrypted passcode values, which can then be reversed due to the use of a weak encryption algorithm. Knowledge of the passcode provides full access to the device functionality. To mitigate this vulnerability, GE is releasing firmware updates that remove the ability to obtain the encrypted passcode values from both the front panel of the device and through the network.

ACKNOWLEDGMENT

The authors would like to acknowledge the GE Product Security Incident Response Team for a productive collaboration during the disclosure of the vulnerability. Furthermore, the authors would like to acknowledge Marios Sazos from the Center for Cyber Security at New York University Abu Dhabi for his assistance in this project.

REFERENCES

[1] ICS-CERT, *Advisory ICSA-17-117-01A: GE Multilin SR, UR, and URplus Protective Relays (Update A)*, 2017

[2] NIST, *Guide to Industrial Control Systems (ICS) Security Revision 2*, 2015