SUMMARY REPORT

GENEREX CS141 CYBER SECURITY TESTING

GENEREX
18610 Starcreek Dr, Suite D, 28031 Cornelius, North

Attn: Mr. Daniel Baileys, TPOC

DOCUMENT NO
2257-001-D002

COMPILED BY
EWA-Canada, An Intertek Company

PROJECT NAME
Generex CS141 Cyber Security Testing

DATE
7 March 2024

List of revisions

REV.	DATE	REVISION DETAILS	AUTHOR	QA/REVIEW	APPROVED
v1.0	29 March 2023	Initial release of report	ZC, WT	BC/WC	SJ
v1.1	28 April 2023	Update to identify whether issues are in the default configuration.	WT	BC	SJ
v1.2	1 March 2024	Update to confirm previous identified vulnerabilities are mitigated.	ZC	WC	SJ

Issuing office: Electronic Warfare Associates – Canada, Ltd., An Intertek Company (“Intertek”) **Disclaimer**

This report has been prepared for the titled project or named part thereof and should not be relied upon or used for any other project without an independent check being carried out as to its suitability and prior written authority of Intertek being obtained. Intertek accepts no responsibility or liability for the consequences of this document being used for a purpose other than the purposes for which it was commissioned. Any person using or relying on the document for such other purposes agrees and will by such use or reliance be taken to confirm his agreement to indemnify Intertek for all loss or damage resulting therefrom. Intertek accepts no responsibility or liability for this document to any party other than the person by whom it was commissioned.

EWA-Canada Location

OTTAWA, ON

1223 Michael St. North,
Suite 200
Ottawa, Ontario, Canada
K1J 7T2

Tel (613) 230-6067
Fax (613) 230-4933

EXECUTIVE SUMMARY

Introduction

Generex has developed the CS141 Web Manager system. This system includes multiple models such as the BACS Webmanager Budget, CS141LM, and CS141L. These models support the management and operation of UPS devices. They perform activities via serial interfaces, with RS232 and RS485 signalling. Additionally, the devices contain a LAN ethernet interface to provide access to the web management interface.

Optionally, administrator users can utilize various other networking services such as SFTP, SMTP, HTTP(s), SNMP, NTP, Modbus TCP, and BACnet IP.

Generex requested a retest of prior issues identified in the penetration test to confirm mitigation.

Scope of Review

This work includes the malformed input testing, structured penetration testing, and retesting previously identified issues.

Summary of Results

The network-based penetration testing against the devices was performed and multiple issues were identified in the initial assessment. The client provided an updated firmware which contained mitigations to the previously identified issues, which were related to the use of default passwords, insecure protocols, insecure configurations, and weak password protection of stored credentials. One informational issue still affects the devices where insecure settings may continue to transfer during regular update procedures.

Fuzzing was performed on the RS232 and RS485 interfaces which included various protocols such as ModBus serial (COM2), ModBus TCP (LAN), SensorManager II (COM2), HTTP (LAN), and SMT_H_COM (COM2). Over the course of this fuzzing, no specific frames were found to cause undesirable or unexpected behaviour on the devices. COM1 interface fuzzing was omitted due to a lack of provided protocol specifications.

Figure 1 – Summary of Results

Severity	Number of Issues
High	0
Medium	0
Low	0
Informational	1

Conclusions

Overall, all but one issue was successfully mitigated. The only issue that continues to affect the devices is an informational issue where insecure settings may continue to transfer during regular update procedures. Over the course of the malformed input testing no sequence was identified that would cause the devices to behave in an undesirable or unexpected manner.

The security assessment and testing results presented in this report simply detail the security posture at a point in time and the ongoing difficulty lies in maintaining the security of the system as improvements are implemented and as the system evolves. Therefore, the key to maintaining the integrity of the device's security posture over time will be to ensure that it is supported by sound, pro-active security processes and procedures.

TABLE OF CONTENTS

LIST OF TABLES

1 INTRODUCTION

1.1 Background

Generex has developed the CS141 Web Manager system. This system includes multiple models such as the BACS Webmanager Budget, CS141LM, and CS141L. These models support the management and operation of UPS devices. They perform activities via serial interfaces, with RS232 and RS485 signalling. Additionally, the devices contain a LAN ethernet interface to provide access to the web management interface. Optionally, administrator users can utilize various other networking services such as SFTP, SMTP, HTTP(s), SNMP, NTP, Modbus TCP, and BACnet IP. Generex requested a retest of prior issues identified in the penetration test to confirm mitigation.

1.2 Purpose

The purpose of this work is to perform security testing and analysis for the CS141 Web Manager system and identify security relevant findings and confirm mitigations.

1.3 Scope

This work includes the malformed input testing and structured penetration testing. Additionally, retesting to determine if the following identified issues have been mitigated:

1. Default credentials were identified in product manuals that are available online;
2. The SNMP service listening on the devices is version 2c and is using the default community string “public”. SNMPv2c only provides simple authentication and does not involve any encryption;
3. Multiple vulnerabilities have been reported to affect the version of OpenSSH, which can be enabled by users;
4. If the ‘Serial Trace’ service is enabled by a user on the device, it accepts connections encrypted using the TLS 1.0 and 1.1 protocol; and
5. If SFTP is enabled by the user, and the user is authenticated as the admin user to the SFTP service on the devices, access to files containing application user password hashes were identified.

1.4 Document Overview

The contents of the remaining sections of this document are as follows:

a. Section 2. This section describes the approach taken to conduct the work.
b. Section 3. This section provides conclusions derived from the work.

2 VA METHODOLOGY

This section describes the methodology used to perform each of the required tasks. This is followed by a description of the rationale behind assigning severity ratings to the security issues. EWA-Canada testing methodology is based on the following industry-recognized best practices:

a. The Open Source Security Testing Methodology Manual;
b. U.S. NIST SP 800-115 - Technical Guide to Information Security Testing and Assessment; and
c. UL 2900-1 Software Cyber Security for Network-Connectable Products.

2.1 Malformed Input testing Methodology

Malformed input testing was performed against the LAN, RS232, and RS485 interfaces on all available protocols.

Testing was conducted on devices running the following software versions:

- Version: CS141-SNMP V2.12.12 221214;
- Backend: v2.10 (ups v1457, bacs v0.4.53); and
- Frontend: v2.4.5 (screens v0.1.93).

Hardware components used in the testing included:

a. VA computer running Ubuntu Linux;
b. VA computer running Kali Linux;
c. Picoscope 3206D;
d. DTECH USB to RS485 Cable HD-link Serial Adapter DB9; and
e. TIAO USB Multi-Protocol Adapter (TUMPA).

Software components used in the testing included:

a. Ubuntu Linux 5.19.0-35-generic;
b. Kali Linux 6.0.0-kali3-amd64;
c. Synopsis Defensics v2022.6.2;
    a. Ethernet Test Suite v5.2.0;
    b. IPv4 Test Suite v6.0.0;
d. Boofuzz Framework v0.4.1;
e. Python v3.10; and
f. Picoscope 6 software.

2.2 Structured Penetration Testing Methodology

Testing was conducted on devices running the following software versions:

- Version: CS141-SNMP V2.12.12 221214;
- Backend: v2.10 (ups v1457, bacs v0.4.53); and
- Frontend: v2.4.5 (screens v0.1.93).

Hardware components used in the testing included:

a. VA computer running Kali Linux; and

b. VA computer running Ubuntu Linux.

Software components used in the testing included:

a. Ubuntu Linux 5.19.0-35-generic;
b. Kali Linux 6.0.0-kali3-amd64;
c. Nessus Version 10.4.2 (#93) LINUX – Policy Template Version 202301231642;
d. Burp Suite Professional v2023.1.2;
e. Nmap 7.93;
f. Netcat 7.93;
g. Wireshark v3.6.2;
h. Ssh-audit v2.5.0;
i. Metasploit 6.3.4-dev;
j. Snmp-check v1.9;
k. Wappalyzer 6.10.55;
l. Dirb v2.22;
m. Ffuf v1.1.0;
n. Hashcat 6.2.6;
o. Ntpd ntpsec-1.2.1; and
p. SSLscan 2.0.15-static.

The assessment of the devices was performed in a manner that ensured that they were tested in their default configurations. In addition, testing on optional services was performed. The following activities were performed against devices:

a. Port Scanning. Nmap and Nessus were used to scan TCP and UDP ports and the IP protocols listening on the target system to identify which services were available.

b. Protocol Fingerprinting and Banner Grabbing. Nmap, Netcat, Metasploit, Snmp-check, and Nessus were used to scan the targets in an attempt to identify details of the remote operating system and any accessible network services.

c. Web Service Scanning. Nessus, Burp Suite Professional, Dirb , Ffuf, and Firefox with the Wappalyzer extension were used to collect information and identify any potentially vulnerable web services on the devices.

d. Vulnerability Scanning. Nessus and Burp Suite were used to conduct comprehensive vulnerability scans of the target. These tools operate in an automated fashion in which the operator identifies the IP addresses of the target, and the output of the tool identifies suspected vulnerabilities in the target devices.

e. Verification of Vulnerabilities. Manual testing with Burp Suite and Google Chrome was conducted to verify the vulnerabilities that were identified by the automated and semi-automated tools, and to identify other vulnerabilities and issues that were not reported by the automated tools.

2.3 Retesting

Retesting was conducted on devices running the following software versions:

- Version: CS141-SNMP V2.18.51 240209;
- Backend: v2.20 (ups v1507, bacs v0.4.54); and
- Frontend: v2.5.0 (screens v0.2.20).

Hardware components used in the testing included:

a. VA computer running Kali Linux.

Software components used in the testing included:

a. Kali Linux 6.0.0-kali3-amd64; and
b. Nmap 7.93.

The retest of the previously identified issues was performed subsequent to updating the devices using installation instructions from the client. The following activities were performed against devices to determine whether issues had been mitigated:

a. Port Scanning. Nmap was used to scan TCP and UDP ports and the IP protocols listening on the target systems to identify which services were available by default.

b. Verification of Vulnerabilities. Manual testing with Firefox was conducted to verify the identified vulnerabilities had been mitigated.

2.4 Severity Ratings

When assigning security issue severities, the following is taken into account:

a. the characteristics of the issue itself;
b. how accessible it is to un-trusted individuals; and
c. the specific operational environment (including other protective mechanisms).

The proposed severity rating assigned by a tool is not relied on to assess priority.

The purpose of this report is to identify and document security issues that have been discovered during this engagement. Typically, “knowledgeable” testing is conducted to identify security issues to be more thorough, accurate, and cost effective. Nonetheless, given sufficient time, an attacker could be expected to discover most of the vulnerabilities. Therefore, in keeping with Information Technology Security best practices, “security by obscurity” by itself is not considered a reasonable risk mitigation approach and a severity rating is assessed based on the security issue itself and is not reflective of how the issue was identified.

In order to indicate the relative severity of each issue, items are categorized using a four-level rating as described in Table 1.

Table 1 – Results Severity Classification

Severity	Description
High	Vulnerability-related Issue The identified issue could be exploited by an un-trusted individual to compromise the system under review. There are no security or protective mechanisms in place that will mediate exploitation of this vulnerability by an un-trusted individual. Design-related Issue The identified issue has a significant negative impact on the ability of the organization to provide services and maintain the security of data. Should be resolved as soon as possible.
Medium	Vulnerability-related Issue The identified issue could be exploited to compromise the system or information under review, however, as there are security or protective mechanisms limiting access to this vulnerability (e.g., firewall, authentication, etc.), the issue is not normally directly accessible to an un-trusted individual. Design-related Issue The identified issue could have a negative impact on the ability of the organization to provide services and maintain the security of data. Should be resolved when resources are available.
Low	Vulnerability-related Issue The identified issue is not directly exploitable, but best IT security practices recommend that the issue should be addressed if possible. Design-related Issue Best practices recommend that the organization consider addressing the identified issue in future development and implementation activities.
Information	Informational issues are provided to indicate where an attacker could gather certain information that could be used to augment knowledge of the system or application or be used in conjunction with other information or vulnerabilities to increase the likelihood of a successful attack.

3 CONCLUSIONS

This work includes the malformed input testing, structured penetration testing, and retesting to confirm mitigations.

Overall, all but one issue was successfully mitigated. The only issue that continues to affect the devices is an informational issue where insecure settings may continue to transfer during regular update procedures. Over the course of the malformed input testing, no sequence was identified that would cause the devices to behave in an undesirable, or unexpected manner.

Nonetheless, the security assessment and testing results presented in this report simply detail the security posture at a point in time and the ongoing difficulty lies in maintaining the security of the system as improvements are implemented and as the system evolves. Therefore, the key to maintaining the integrity of the device's security posture over time will be to ensure that it is supported by sound, pro-active security processes and procedures.

Figure 1 – Summary of Results

Severity	Number of Issues
High	**0**
Medium	**0**
Low	**0**
Informational	**1**

Table 4 – Issues and Recommendations Table

No	Issues and Recommendations
1	**Priority:** Informational **Issue:** Insecure settings may be migrated across updates as normal update procedures.