The POWER PULSE UTILITIES

Vulnerability Assessment Review

11/8/2024

Frederic Gariepy

Table of Contents

Executive Summary..... 2
Introduction..... 2
Identification of Vulnerabilities..... 3
Analysis Using Vulnerability Databases..... 3
Determination of Exploitability..... 4
Impact Analysis..... 4
Contextualization..... 5
Threat Environment..... 6
Prioritization..... 6
Plan of Action..... 7
Conclusion..... 7
References..... 8

Executive Summary

A total of 3 vulnerabilities were assessed based on the Jan 4th, 2024 Vulnerability Scan Report for POWER PULSE UTILITIES.

Key Insights:

- All found vulnerabilities have official fixes of low complexity, requiring software updates and (regularly) applying security patches.
- A critical vulnerability is present on 40 employee work desktop and laptops, with an official fix being a software update.
- A high severity vulnerability is present on 6 Siemens Remote Terminal Units (RTUs) spread over 3 distribution stations, with an official fix being a software update.
- A medium severity vulnerability is present on 35 SIP phones spread over the head offices, with an official fix being a software update.

Consult the Prioritization and Plan of Action sections for immediate remediations of vulnerabilities found.

Consult the Conclusion section for further document overview and recommendations.

Introduction

This report represents an analysis of the current security vulnerabilities identified across POWER PULSE UTILITIES' Information Technology (IT) and Operational Technology (OT) environments. The vulnerabilities identified in the scan report have been further assessed considering the compensating controls in POWER PULSE UTILITIES' environment and the potential impacts if these vulnerabilities were to be exploited. Recommendations have also been made for each vulnerability to remediate and/or mitigate the risks associated with these vulnerabilities.

Vulnerabilities overview:

Severity Category	Low	Medium	High	Critical
Vulnerability Count	0	1	1	1

Identification of Vulnerabilities

The following section is based on the Jan 4th, 2024 Vulnerability Scan Report for POWER PULSE UTILITIES.

The scan produced these vulnerabilities:

Vulnerability Index	Severity Category	Vulnerability Name
1	Critical	**Zoom Client for Meetings < 5.15.2 Vulnerability (ZSB-23038) (CVE-2023-39213)**
2	High	**Siemens (CVE-2023-42797)**
3	Medium	**Cisco IP Phone Stored XSS (cisco-sa-uipphone-xss-NcmUykqA)**

Analysis Using Vulnerability Databases

After review of vulnerabilities based on NIST NVD and CVSS 3.1, the following was discovered:

Vulnerability 1:
Zoom Client for Meetings < 5.15.2 Vulnerability (ZSB-23038) (CVE-2023-39213).
Improper neutralization of special elements in Zoom Desktop Client for Windows and Zoom VDI Client before 5.15.2 may allow an unauthenticated user to enable an escalation of privilege via network access. The vendor solution is to apply current updates or download the latest Zoom software.

CVSS v3.1 Base score of: 9.8, or Critical.

Vulnerability 2:
Siemens (CVE-2023-42797).
The CPCI85 firmware of SICAM A8000 CP-8031 and CP-8050 is affected by a command injection vulnerability that could allow an authenticated remote attacker to inject commands that are executed on the device with root privileges during device startup. Siemens has released new versions for the affected products and recommends updating to the latest versions.

CVSS v3.1 Base score of: 7.2, or High.

Vulnerability 3:
Cisco IP Phone Stored XSS (cisco-sa-uipphone-xss-NcmUykqA)(CVE-2023-20265)
A vulnerability in the web-based management interface of a small subset of Cisco IP Phones could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. An attacker with valid credentials and access the web-based management interface of the affected device could execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Cisco has released software updates that address this vulnerability.

CVSS v3.1 Base score of: 5.4, or Medium.

Determination of Exploitability

Vulnerability 1:
Zoom Client for Meetings < 5.15.2 Vulnerability (ZSB-23038) (CVE-2023-39213).
No known exploits are available, as indicated by Tenable's plugin entry for this vulnerability.
CVSS v3.1 Base score of: 9.8, or Critical.
The Attack Vector is Network based, the Attack Complexity is Low, Privileges are Not required, and User Interaction is Not Required.

Vulnerability 2:
Siemens (CVE-2023-42797).
No known exploits are available, as indicated by Tenable's plugin entry for this vulnerability.
CVSS v3.1 Base score of: 7.2, or High.
The Attack Vector is Network based, the Attack Complexity is Low, Privileges required is High, and User Interaction is Not Required.

Vulnerability 3:
Cisco IP Phone Stored XSS (cisco-sa-uipphone-xss-NcmUykqA)(CVE-2023-20265)
No known exploits are available, as indicated by Tenable's plugin entry for this vulnerability.
CVSS v3.1 Base score of: 5.4, or Medium.
The Attack Vector is Network based, the Attack Complexity is Low, Privileges required is Low, and User Interaction is Required.

Impact Analysis

Vulnerability 1:
Zoom Client for Meetings < 5.15.2 Vulnerability (ZSB-23038) (CVE-2023-39213).
Vulnerability exists across all 40 work desktops used regularly by employees which contain confidential operational information and client information. The vulnerability impact poses a high risk to confidentiality, integrity and availability.

Vulnerability 2:
Siemens (CVE-2023-42797).
The vulnerability exists across 6 Siemens Remote Terminal Units (RTUs) spread over 3 distribution stations. The environment of the vulnerability requires the attacker to have local network access to exploit the vulnerability and inject commands executed with root privileges. The vulnerability impact poses a high risk to confidentiality, integrity and availability.

Vulnerability 3:
Cisco IP Phone Stored XSS (cisco-sa-uipphone-xss-NcmUykqA)(CVE-2023-20265).
The vulnerability exists across 35 SIP phones (model 3905) spread over the head offices. These devices are not in regular use and do not contain sensitive information. The vulnerability could be used to leverage sophisticated phishing attacks. The vulnerability impact poses a low risk to confidentiality, integrity and availability.

Contextualization

Vulnerability 1:
Zoom Client for Meetings < 5.15.2 Vulnerability (ZSB-23038) (CVE-2023-39213).
Devices affected by vulnerability are used regularly by employees. Devices consist of desktops and laptops. The laptops contain confidential operational information, and some may contain confidential client information. The high requirement for confidentiality, integrity, and availability of the information makes this vulnerability urgent to solve.

The CVSS 3.1 calculator was used to calculate an environmental score for this vulnerability. The environmental severity of this vulnerability is 8.5 (High).

https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C/CR:H/IR:H/AR:H

Vulnerability 2:
Siemens (CVE-2023-42797).
The 6 Siemens RTUs at Power Pulse's 3 distribution stations are affected by this vulnerability. These stations are protected by firewalls, requiring any traffic from Power Pulse's wide area networks to pass through a firewall at each station. To exploit this vulnerability, an attacker would need access to the local network within one of the stations, as there is no direct Internet access. Although RTUs have high integrity and availability requirements, the environmental context (MAV: Local) reduces the severity of this vulnerability to medium.

The CVSS 3.1 calculator was used to calculate an environmental score for this vulnerability. The environmental severity of this vulnerability is 6.3 (Medium).

https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C/IR:H/AR:H/MAV:L

Vulnerability 3:
Cisco IP Phone Stored XSS (cisco-sa-uipphone-xss-NcmUykqA)(CVE-2023-20265)
The 32 SIP phones (model 3905) devices at Power Pulse's head office are not used often in day-to-day operations, where instead employees use corporate cell phones or the Zoom client on their computers. All calls from clients are routed to a separate call center operated by a third-party organization. The devices are considered of low importance from a confidentiality, integrity, and availability perspective.

The CVSS 3.1 calculator was used to calculate an environmental score for this vulnerability. The environmental severity of this vulnerability is 3.5 (Low).

https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N/E:U/RL:O/RC:C/CR:L/IR:L/AR:L

Threat Environment

AS per the November 2020 Cyber threat bulletin “cyber threat actors likely view Canada as an intermediate target through which they can impact the US electricity sector” (Goverment of Canada, 2020). This observation has been exacerbated over the past 4 years through geopolitical events, such as the Russia’s invasion of Ukraine in 2022, growing cyber threat programs and state-sponsored threat actors from the PRC, Russian Federation, Islamic Republic of Iran, DPRK, and the Republic of India according to the National Cyber Threat Assessment 2025-2026 (Goverment of Canada, 2024).

The observation of Canada as an intermediary to threats against the US has demonstrable effects, as “all 10 U.S. energy companies were included in confirmed third-party breaches” and 90% of affected energy companies were breached through third-party attacks (Nadeau, 2024).

Following the trends and reports, the top cybersecurity threats to Canada's energy sector include state-sponsored cyber activities, ransomware attacks, supply chain compromises, insider threats, and vulnerabilities in industrial control systems (Goverment of Canada, 2024). Canada’s complex energy infrastructure, involving both legacy systems and modern tech, IT and OT creates unique vulnerabilities which must be mitigated with special attention to the threat landscape.

Prioritization.

The table below outlines recommended timelines for remediation of each vulnerability based on the value of affected assets and the nature of each vulnerability within the environmental context.

Vulnerability#	Recommended Implementation Timeframe	Rationale
Vulnerability 1, Zoom Client for Meetings < 5.15.2 Vulnerability (ZSB-23038) (CVE-2023-39213).	Should be remediated as soon as possible, within 24-48 hours.	The vulnerability is a priority since it has the most significant impacts over the organization and can be exploited over the internet with low complexity and low privileges.
Vulnerability 2, Siemens (CVE-2023-42797).	Should be addressed within 14 days.	Vulnerability poses a significant integrity and availability risk that can be exploited by threat actors through insider threats.
Vulnerability 3, Cisco IP Phone Stored XSS (cisco-sa-uipphone-xss-NcmUykqA)(CVE-2023-20265)	Should be addressed within 30 days.	The environmental score puts this vulnerability in low severity. However, the network attack vector with low complexity and low privilege coupled with a back-dated official fix presents an opening for social engineering attacks, and the base score indicates the vulnerability to be of moderate severity.

Plan of Action

All vulnerabilities highlighted in this document have official fixes, all of which should be followed as per instructions found here and by vendor's directions.

Vulnerability 1,
Zoom Client for Meetings < 5.15.2 Vulnerability (ZSB-23038) (CVE-2023-39213).
Vendor directs to apply current updates or download the latest Zoom software with all current security updates from https://zoom.us/download. (Zoom, 2023)

Vulnerability 2,
Siemens (CVE-2023-42797).
Siemens has released new versions for the affected products and recommends updating to the latest versions. Update to CPCI85 V05.20 or later version
https://support.industry.siemens.com/cs/ww/en/view/109804985/." (Siemens, 2024)

Vulnerability 3,
Cisco IP Phone Stored XSS (cisco-sa-uipphone-xss-NcmUykqA)(CVE-2023-20265)
Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability. (Cisco, 2023)

Conclusion

This vulnerability assessment has revealed a critical, a high, and a medium severity vulnerability in POWER PULSE UTILITIES' environment. These vulnerabilities, if left unchecked, could potentially lead to unauthorized access, data breaches, facilitation of third-party threat, and other security incidents that could have an impact severe impact on operations.

The most critical vulnerability discovered is a Zoom Client for Meetings Vulnerability on employee work desktop and laptops. This vulnerability should be patched with the official vendor fix through software update in the next 24-48 hours.

The other two vulnerabilities should be patched as well on a schedule that aligns with POWER PULSE UTILITIES' Vulnerability Management standard.

Considering the date of each vulnerability publication in the NVD and the date of official fixes available for these vulnerabilities are dated to last year, it is recommended that POWER PULSE UTILITIES ought to strengthen its software update and security patch enforcement policies in order to stay resilient in the face of cyber threats and compliant with its internal and external policies.

References

Cisco. (2023, 11 15). *Cisco IP Phone Stored Cross-Site Scripting Vulnerability*. From Cisco: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-uipphone-xss-NcmUykqA

Goverment of Canada. (2020). The cyber threat to Canada's electricity sector. *Cyber threat bulletin.*

Goverment of Canada. (2024). National Cyber Threat Assessment 2025-2026. *Canadian Centre for Cyber Security*.

Nadeau, J. (2024, 2 6). *Third-party breaches hit 90% of top global energy companies*. From Security Intelligence: https://securityintelligence.com/articles/third-party-breaches-top-global-energy-companies/

Siemens. (2024, 9 1). *SSA-583634: Command Injection Vulnerability in the CPCI85*. From Siemens Security Advisory by Siemens ProductCERT: https://cert-portal.siemens.com/productcert/pdf/ssa-583634.pdf

Zoom. (2023, 8 8). *Zoom Desktop Client for Windows and Zoom VDI Client - Improper Neutralization of Special Elements*. From Zoom: https://www.zoom.com/en/trust/security-bulletin/zsb-23038/