**The POWER PULSE UTILITIES** 

# **Vulnerability Assessment Report 2024**

November 11, 2024

Seran Sathyaseelan

## Executive Summary

This report provides a comprehensive analysis of three identified vulnerabilities from a recent vulnerability scan performed on Power Pulse Utilities' infrastructure. The vulnerabilities have been assessed with environmental factors specific to Power Pulse’s operations in mind. The report highlights the risks, recalculated CVSS v3.1 environmental scores, and recommended mitigation timeframes for each vulnerability to safeguard operational integrity, minimize risk, and ensure business continuity.

## Introduction

Power Pulse Utilities is responsible for delivering reliable power distribution to 30,000 residents across residential, commercial, and light industrial sectors. Following a vulnerability scan performed by a third-party consulting firm, three vulnerabilities were identified that could potentially impact Power Pulse’s IT and OT systems. This document provides:

* A detailed analysis of each vulnerability.
* The recalculated CVSS v3.1 Environmental Scores tailored to Power Pulse's environment.
* Recommended implementation timeframes for remediation based on risk severity.  
  The goal is to prioritize mitigation efforts to ensure confidentiality, integrity, and availability (CIA) of critical systems and data.

## Identification of Vulnerabilities

After reviewing vulnerability scan done by the third-party consulting company hired by Power Pulse, 3 vulnerabilities were discovered.

**Vulnerability #1**- [Zoom Client For Meetings **5.15.2** Vulnerability (ZSB-23038)](https://www.tenable.com/plugins/nessus/184369)

**Vulnerability #2** – [Siemens (CVE-2023-42797)](https://www.tenable.com/plugins/ot/501888)

**Vulnerability #3** – [Cisco IP Phone Stored XSS (cisco-sa-uipphone-xss-NcmUykqA)](https://www.tenable.com/plugins/nessus/186612)

## Analysis Using Vulnerability Databases

Using Tenable, CVSS and other platforms an analysis was done to provide more insight on each vulnerability. The following provides more details on the findings:

**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 current solution according to Tenable is to upgrade to Zoom Client for Meetings 5.15.2 or later.
* CVSS v3.1 base score is 9.8 or Critical

**Vulnerability #2** – Siemens (CVE-2023-42797)

* A vulnerability has been identified in **CP-8031 MASTER MODULE** (All versions < CPCI85 V05.20**), CP-8050 MASTER MODULE** (All versions < CPCI85 V05.20). The network configuration service of affected devices contains a flaw in the conversion of ipv4 addresses that could lead to an uninitialized variable being used in succeeding validation steps.  
  By uploading specially crafted network configuration, an authenticated remote attacker could be able to inject commands that are executed on the device with root privileges during device startup.
* Currently the vendor advisory for mitigation includes the following
  + update to CPCI85 V05.20 or later version
  + Review the list of users that are allowed to modify the network configuration and apply strong passwords
* CVSS v3.1 base score is 7.2 or High

**Vulnerability #3-** Cisco IP Phone Stored XSS (cisco-sa-uipphone-xss-NcmUykqA) (CVE-2023-20265)

* According to its self-reported version, Cisco IP Phone Stored Cross-Site Scripting may be affected by a cross-site scripting (XSS) vulnerability. Due to insufficient validation of user-supplied input, an authenticated, remote attacker can conduct an XSS attacker against a user of the interface on the affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker must have valid credentials to access the web-based management interface of the affected device.
* The current solution according to Tenable is to upgrade to the relevant fixed version referenced in [Cisco bug](https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-uipphone-xss-NcmUykqA) IDs **CSCwf58592**, **CSCwf58594**
* CVSS v3.1 base score is 5.4 or Medium

## Determination of Exploitability

**Vulnerability #1**- Zoom Client for Meetings **5.15.2** Vulnerability (ZSB-23038) (CVE-2023-39213)

* No exploits are currently available for this vulnerability
* CVSS v3.1 base score is 9.8 or Critical
* Exploitability metrics is as follows
  + **Attack Vector:** Network
  + **Attack Complexity:** Low
  + **Privileges:** None
  + **User Interaction:** None
  + **Scope:** Unchanged

**Vulnerability #2** – Siemens (CVE-2023-42797)

* No exploits are currently available for this vulnerability
* CVSS v3.1 base score is 7.2 or High
* Exploitability metrics is as follows
  + **Attack Vector:** Network
  + **Attack Complexity:** Low
  + **Privileges:** High
  + **User Interaction:** None
  + **Scope:** Unchanged

**Vulnerability #3-** Cisco IP Phone Stored XSS (cisco-sa-uipphone-xss-NcmUykqA) (CVE-2023-20265)

* No exploits are currently available for this vulnerability
* CVSS v3.1 base score is 5.4 or Medium
* Exploitability metrics is as follows
  + **Attack Vector:** Network
  + **Attack Complexity:** Low
  + **Privileges:** Low
  + **User Interaction:** Required
  + **Scope:** Changed

## Impact Analysis

After assessing the vulnerabilities, the impact of such vulnerabilities was determined as follows:

**Vulnerability #1**- Zoom Client for Meetings **5.15.2** Vulnerability (ZSB-23038) (CVE-2023-39213)

This software is installed on all 40 Windows desktops and laptops that Power Pulse employees use. This contains confidential information regarding Power Pulse’s operations as well as confidential client information. An improper neutralization of special elements and the potential escalation of privileges via network access means that there is a potential loss or compromise of sensitive personal and business data. This can lead to ransomware attacks, disruptions in day-to-day operations and reputational damage to name a few.

**Vulnerability #2** – Siemens (CVE-2023-42797)

The Siemen remote terminal units (RTUs) are located at Power Pulse’s 3 distribution stations with each having its own firewall protection as well as no internet access. Despite this, the flaw in the conversion of ipv4 addresses could lead to privilege escalation, supply chain attacks, Dos attacks and even remote code execution. However, its worth noting that because of the firewall and no access to the internet at each station, an external threat actor cannot reach systems directly and therefore need physical access to the stations or comprise a device that’s already inside the internal network. The multiple layers of protection significantly reduce the potential risk of this vulnerability being exploited.

**Vulnerability #3-** Cisco IP Phone Stored XSS (cisco-sa-uipphone-xss-NcmUykqA) (CVE-2023-20265)

This vulnerability affects 35 SIP phones located at Power Plue’s head office. These phones are all routed to a separate call center operated by a third-party organization. The stored XSS attack that can result from this vulnerability can lead to not just to comprise of user and administrator accounts but also create a potential entry point for broader attacks. This could lead to network comprise if a threat actor were to move laterally within the company. However, it’s worth noting that due to the limited use of the SIP phones by employees the devices are viewed as low importance from a CIA triad perspective.

## Contextualization

With the vulnerabilities identified, the following section provides a more in-depth analysis of each vulnerability within the Power Pulse environment. Environmental considerations have been factored in to recalculate the CVSS v3.1 scores, offering a tailored assessment of their criticality.

**Vulnerability #1**- The Zoom Client for Meetings vulnerability poses a significant risk as it requires no user interaction and can be exploited over the network. This makes it easier for an attacker to gain access to highly sensitive business and client information stored on the affected systems. While the software is installed on all 40 Windows laptops, its exploitation would not result in a catastrophic outage to business operations but would still hinder productivity and expose sensitive data.

Considering these environmental factors, the CVSS v3.1 Environmental Score is recalculated as 8.5 (Critical), reflecting the severity of the risk in Power Pulse's operational environment.

**Vulnerability #2** - Siemens (CVE-2023-42797)

The 6 Siemens RTUs located across Power Pulse’s 3 distribution stations are crucial for maintaining power distribution. The primary concern is the availability of these systems, as any disruption could severely impact business operations. However, confidentiality is of lower importance since the RTUs store only operational data, not sensitive information.

Multiple layers of protection are in place, including firewalls and the absence of internet access, which limit exposure to external attacks. Therefore, the Attack Vector can be modified from Network to Local, as a threat actor would need local network access to exploit this vulnerability. With these environmental considerations factored in, the recalculated CVSS v3.1 Environmental Score is 5.8 (Medium), reflecting a moderate risk.

**Vulnerability #3-** Cisco IP Phone Stored XSS (cisco-sa-uipphone-xss-NcmUykqA) (CVE-2023-20265)

The Cisco IP Phone vulnerability impacts 35 SIP phones located at Power Pulse’s head office. These phones are deemed of low importance as they are rarely used by employees, who rely more on corporate cell phones and the Zoom client for communication. Additionally, phones do not play a critical role in business operations. Given the limited usage and impact, the recalculated CVSS v3.1 Environmental Score is 5.4 (Medium), underscoring the low severity of this vulnerability within Power Pulse’s environment. Threat Environment

## Prioritization.

The vulnerabilities have been prioritized based on their risk severity, asset criticality, and potential impact on Power Pulse’s operations.

|  |  |  |
| --- | --- | --- |
| **Vulnerability#** | **Recommended Implementation Timeframe** | **Rationale** |
| Zoom Client for Meetings **5.15.2** Vulnerability (ZSB-23038) (CVE-2023-39213) | 24-48 hours | Confidential client information and sensitive Power Pulse operational data mean this vulnerability must be addressed immediately to prevent data loss, potential lawsuits, and reputational damage. |
| Siemens (CVE-2023-42797) | 14 days | Siemens RTUs are critical for maintaining power distribution, and availability is the primary concern. While protections like firewalls limit external exposure, addressing this vulnerability promptly will mitigate potential operational disruptions caused by local access exploitation. |
| Cisco IP Phone Stored XSS (cisco-sa-uipphone-xss-NcmUykqA) (CVE-2023-20265) | 30 days | The Cisco SIP phones are of low importance and are rarely used, making this vulnerability low priority. Addressing it within 30 days ensures best practices are maintained without significant operational impact. |

## Plan of Action

The Zoom Client for Meetings 5.15.2 vulnerability (CVE-2023-39213), with an environmental score of 8.5 (Critical), must be addressed within 24-48 hours. This vulnerability requires no user interaction and can be exploited over the network, posing a significant risk to confidential business and client information stored on Power Pulse’s 40 Windows laptops and desktops. The remediation plan involves upgrading all Zoom Clients to version 5.15.2 or later, testing the update for functionality, and communicating the changes to employees to ensure proper installation and operation. Post-remediation, systems will be monitored for anomalies, and compliance will be validated to confirm that all devices are updated. Given the sensitivity of the data, immediate action is necessary to prevent potential breaches, legal liability, and operational disruptions.

The Siemens RTU vulnerability (CVE-2023-42797), with an environmental score of 5.8 (Medium), should be resolved within 14 days to ensure operational continuity. The 6 Siemens RTUs located across Power Pulse’s 3 distribution stations are critical for maintaining power distribution, making availability the primary concern. While protections like firewalls and restricted internet access mitigate external risks, local network access could still allow exploitation. Remediation steps include applying the latest firmware updates provided by Siemens, strengthening local access controls, and testing the updates in a non-production environment to avoid unintended disruptions. Additionally, network activity will be monitored for unusual behavior, and access controls such as role-based authentication will be reinforced. A 14-day timeframe ensures the vulnerability is addressed promptly without compromising operational stability.

The Cisco IP Phone Stored XSS vulnerability (CVE-2023-20265), with an environmental score of 5.4 (Medium), is of low importance and can be remediated within 30 days. The 35 affected Cisco SIP phones are located at Power Pulse’s head office but are rarely used, as employees primarily rely on corporate cell phones and the Zoom client for communication. To address this vulnerability, the firmware for all Cisco SIP phones will be updated to the latest version recommended by Cisco. Security configurations will be reviewed, and any unnecessary features or services will be disabled to minimize the attack surface. During the process, alternative communication methods will be tested to ensure no operational impact occurs. Limited monitoring will be implemented to detect any unusual activity, and the remediation process will be documented to confirm completion.

## Conclusion

This vulnerability assessment has identified and prioritized three key risks within Power Pulse Utilities’ environment. The findings consider the criticality of affected assets, operational dependencies, and mitigating factors such as firewalls and network isolation. By implementing the recommended remediation actions within the specified timeframes, Power Pulse can significantly reduce its exposure to potential cyber threats while ensuring business continuity and the safety of critical infrastructure.

This report underscores the importance of addressing vulnerabilities in a timely manner, with particular emphasis on Zoom Client vulnerabilities due to their potential to expose sensitive information and disrupt productivity. Siemens RTU vulnerabilities and Cisco IP phone risks, though of lower severity, must also be addressed to maintain the organization’s security posture.