**The POWER PULSE UTILITIES** 

# **Vulnerability Assessment Report**

2024-04-27

OLAJIDE USMAN

## Executive Summary

This report presents findings from a vulnerability assessment of a scan that was conducted in April 2024 by ExpertEdge Consulting Group for PowerPulse Utilities. The goal of this assessment report is to evaluate the security vulnerabilities identified in the scan report, provide an assessment of how these vulnerabilities could potentially impact PowerPulse Utilities from both an exploitability and impact perspective and to recommend actions to remediate or mitigate these vulnerabilities.

Key Insights:

* 3 vulnerabilities in total were identified in the scan report.
* A critical vulnerability was identified in the PowerPulse’s Zoom Client < 5.15.2 for meetings installed on 40 windows desktop computers.
* A high-risk vulnerability was identified in 6 Siemens Remote Terminal Unit (RTU) that is spread across 3 distribution stations. The mitigating controls in place lowered the severity of this vulnerability to a medium.
* A medium risk vulnerability was identified on the CISCO IP Phone Stored XSS.

| **Critical** | **High** | **Medium** | **Low** |
| --- | --- | --- | --- |
| 1 | 1 | 1 | 0 |

This report represents an analysis of the current security vulnerabilities identified across PowerPulse Utilities’s Information Technology (IT) and Operational Technology (OT) environments. The vulnerabilities identified in the scan report have been further assessed considering the compensating controls in PowerPulse’s 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.

## Introduction

The goal is to **proactively**address security flaws, minimize the organization's exposure to potential cyber threats, and enhance overall resilience against attacks.

## Identification of Vulnerabilities

The results from the recent vulnerability scan produced these three vulnerabilities:

* Vulnerability #1 - Zoom Client for Meetings < 5.15.2 Vulnerability (ZSB-23038)
* Vulnerability #2 - Siemens (CVE-2023-42797)
* Vulnerability #3 - Cisco IP Phone Stored XSS (cisco-sa-uipphone-xss-NcmUykqA)

## Analysis Using Vulnerability Databases

Review vulnerability in various sources and present your findings.

After reviewing the three vulnerabilities in NVD and CVSS, this is what was discover

* Vulnerability #1 Zoom Client for Meetings < 5.15.2 Vulnerability (ZSB-23038): The version of Zoom Client for Meetings installed on the 40 desktop and laptops computers is prior to 5.15.2. It is, therefore, affected by a vulnerability as referenced in the ZSB-23038 advisory.  
    
  - 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 Base score as per CVSS v3.0 for this vulnerability 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.

The base score as per CVSS v3.0 for this vulnerability is 7.2 or high

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

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. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by persuading a user of an affected interface to view a page containing malicious HTML or script content. 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 base score as per CVSS v3.0 for this vulnerability is 5.4 or medium.

## Determination of Exploitability

Vulnerability #1

* Exploits are available currently for this vulnerability as per <https://www.tenable.com/plugins/nessus/184369>
* The CVSS v3 Base score is 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

* Exploits are available currently for this vulnerability as per <https://www.tenable.com/plugins/ot/501888>
* The CVSS v3 Base score is 7.2 or high.
* The attack vector is network based, the attack complexity is low, privileges are required, and user interaction is not required.

Vulnerability #3

* Exploits are available currently for this vulnerability as per <https://www.tenable.com/plugins/nessus/186612>
* The CVSS v3 Base score is 5.4 or medium.
* The attack vector is network based, the attack complexity is low, privileges are not required, and user interaction is required.

## Impact Analysis

Vulnerability #1 - Zoom Client for Meetings < 5.15.2 Vulnerability (ZSB-23038): since the 40 windows desktops and laptops are used by the PowerPulse employees and it contains confidential client information and operational trade secret. The sensitive information is at a high risk of being compromised.

Vulnerability #2 - Siemens (CVE-2023-42797): This is a vulnerability in 6 Siemens Remote Terminal units that are located at Power Pulse’s 3 distribution stations. Each is protected by a firewall, so all traffic traveling to the station across Power Pulse’s wide area networks needs to pass through this firewall located at each station. Therefore an attacker would need to get onto the local network to exploit devices located in the 3 stations. Also, Internet access is not available from the station networks. if any of the devices in the stations is compromised it would not have an impact on their production operations.

Vulnerability #3 - Cisco IP Phone Stored XSS (cisco-sa-uipphone-xss-NcmUykqA): This vulnerability is related to a CISCO vulnerability affecting 35 SIP phones (model 3905) that are all located at Power Pulse’s head office. These devices are considered of low importance from a confidentiality, integrity, and availability perspective, as they aren’t used that often since most employees use their corporate cell phones or the Zoom client on their computers to call colleagues. Additionally, all calls from clients are routed to a separate call center operated by a third-party organization. if any of the devices in the stations is compromised it would not have any significant impact on their production operations

## Contextualization

Vulnerabilities should be assessed based on the environment in which the vulnerability resides. For example a vulnerability in a development environment may have a different risk level than the same vulnerability in a production or QA environment.

Business context should be considered, such as the importance of the system from a business process perspective.

Consideration was given to compensating controls that can mitigate risk. The CVSS 3.1 calculator was used to determine an adjusted score for each vulnerability based on the Environmental Scores.

**Vulnerability #1 - Zoom Client for Meetings < 5.15.2 Vulnerability (ZSB-23038):**

The 40 windows desktops and laptops beingg affected by this vulnerability are used by the PowerPulse employees and it contains confidential client information and operational trade secret. The confidentiality, integrity and availability of this 40 systems is very importan.

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:L/IR:H/AR:H>

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

The 6 Siemens RTU are Remote Terminal units being affected by this vulnerability resides in PowerPulses’s 3 distribution stations and are not deployed to production. The confidentialy, integrity and availability reuires for the RTUs are low.

Additionally, there is no internet access at the stations and each is protected with a firewall from the rest of the network so the modified Attack Vector is set to adjacent as an attackee would need to be connecetd to the stations network to exploit this vulnerability.

The overall environmental score is 4.4(medium) which is much lower than the base score which reflectes the fact that these devices are isolated.

The CVSS 3.1 calculator was used to calculate an environmental score for this vulnerability. The environmental severity of this vulnerability is 4.4 (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/CR:L/IR:L/AR:L/MAV:A>

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

The 35SIP Phones affected by this vulnerability are located in the head office and are low importance from a CIA perspective because they are not used that often since most employees make us ef their cellphones or Zoom client and calls from external clients are routed through an external third party. Thus, the environmental metrics support the fact that this vulnerability is not urgent in nature.

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:L/E:U/RL:O/RC:C/CR:L/IR:L/AR:L/MAV:A>

## Threat Environment

The threat landscape for utilities has expanded to include more threats from more actors. Nation-state actors and other sophisticated players have demonstrated greater willingness to target infrastructure providers as part of their broader campaigns. A January 2020 alert from one government source indicated that critical infrastructure providers should beware of nation-states “capable, at a minimum, of carrying out attacks with temporary disruptive effects against critical infrastructure” as a deterrent or retaliatory measure for other geopolitical developments.1

In addition, cybercriminals target utilities and other critical infrastructure players for profit. One of the most public examples of this willingness to disrupt daily life occurred in May 2019, when a ransomware attack disabled Baltimore city computers for weeks, incurring an estimated $18.2 million in damages—more than the demanded ransom.2 The focus of such attacks is no longer limited to IT networks alone; a government agency recently warned that ransomware had been deployed to disrupt a gas company’s visibility into pipeline operations, leading to a loss of productivity and revenue until the ransomware was removed.

## Prioritization Plan of Action

|  |  |  |
| --- | --- | --- |
| **Vulnerability#** | **Recommended Implementation Timeframe** | **Rationale** |
| #1 - Zoom Client for Meetings < 5.15.2 Vulnerability (ZSB-23038) | 24-48 hours | Customer data potentially at risk, 40 Internet facing system, this could result in significant impacts to customer data and impact PowerPulse’s reputation, lead to financial loss and regulatory fines. |
| #2 - Siemens (CVE-2023-42797) | 30 days | Although the 6 RTUs are OT devices and are not critical to PowerPulse’s operations this vulnerability should still be treated as Medium and be patched within 30 days. |
| #3 - Cisco IP Phone Stored XSS (cisco-sa-uipphone-xss-NcmUykqA) | 30 days | Although the Base Metric for the vulnerability is Medium, it should be treated as Medium given the fact that they are not used often by employees and customers calls are routed to their cell phones through a third-party call center and should be patched within 30days. |

## Conclusion

This vulnerability assessment has revealed a critical vulnerability, one high, and one medium vulnerabilities in PowerPulse’s environment. These vulnerabilities, if left unchecked, could potentially lead to unauthorized access, data breaches, and other security incidents that could have an impact on PowerPulse’s operations.

The most critical vulnerability discovered is a Zoom Client for Meetings < 5.15.2 (ZSB-23038) Vulnerability on PowerPulse’s Internet facing employees 40 desktops and laptops. This vulnerability should be patched by ensuring the upgrade to Zoom Client for meetings 5.15.2 or later in the next 24-48 hours.

The other two vulnerabilities should be patched as well on a schedule that aligns with PowerPulse’s Vulnerability Management standard.