**The POWER PULSE UTILITIES**

# **VULNERABILITY ASSESSMENT REPORT**

7th April, 2024.

Prepared by: Indo Bishmang.

## Executive Summary

This report details the results of a vulnerability assessment conducted by Power Pulse Utilities on April 5th, 2024. The objective of this assessment report is to assess the security vulnerabilities identified within Power pulse’s systems and network infrastructure. It examines these vulnerabilities from both exploitability and impact perspectives and suggests potential mitigation strategies.

Key Insights:

* 3 vulnerabilities in total were identified in the scan report.
* A critical vulnerability was identified in the power pulse video conferencing web application
* A high-risk vulnerability was identified in a Siemens Remote Terminal Unit (RTU). The mitigating controls in place lowered the severity of this vulnerability to a medium.
* A medium risk vulnerability was identified on the CISCO 3905 model of the SIP phone with 35 phones affected and are being used at the corporate office.

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

This report provides an examination of the existing security vulnerabilities detected within Power pulse's Information Technology (IT) and Operational Technology (OT) environment. The vulnerabilities highlighted in the scan report have undergone additional evaluation, taking into account the compensating controls within Power pulse's environment and the potential consequences if these vulnerabilities were to be exploited. Furthermore, recommendations have been outlined for addressing and/or reducing the risks linked with each vulnerability.

## Introduction

Purpose:

* Identify vulnerabilities in networked systems, applications and infrastructure.
* Evaluate the potential impact of discovered vulnerabilities to business operations.
* Provide actionable recommendations to mitigate risk associated with vulnerabilities.

Scope:

* The assessment covered systems, infrastructure and applications in Power Pulse’s Operational Technology (OT) and Information Technology (IT) environments.

## Identification of Vulnerabilities

The following vulnerabilities below were discovered after a vulnerability scan was provided by a third-party security company hired by Power pulse.

* <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) **CVE-2023-20265**

## Analysis Using Vulnerability Databases

A thorough review of vulnerabilities in various sources was conducted including, [Tenable’s Vulnerability Plug-In Database](https://www.tenable.com/plugins), [NIST’s National Vulnerability Database](https://nvd.nist.gov/) and [CISA’s Cybersecurity Alerts & Advisories](https://www.cisa.gov/news-events/cybersecurity-advisories) site.

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

As per CVE-2023-39213, The version of Zoom Client for Meetings installed on the remote host is prior to 5.15.2. ‘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’ i.e. higher levels of access could be gained from anywhere over the network.

The CVSS v3 base score for this vulnerability is 9.8 and the temporal score is 8.5 which results in this vulnerability being rated as CRITICAL.

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

A vulnerability has been identified in CP-8031 MASTER MODULE (All versions < CPCI85 V05.20), CP-8050 MASTER MODULE (All versions < CPCI85 V05.20). A flaw in the conversion of IP addresses has been found in the configuration of affected devices, this could lead to a remote unauthenticated attacker having access to inject commands that can take effect with root privilege at device startup.

The CVSS v3 base score for this vulnerability is 7.2 and the temporal score is 6.3 which results in this vulnerability being rated as HIGH.

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

As per CVE-2023-20265, Cisco IP Phone Stored Cross-Site Scripting may be affected by a cross-site scripting (XSS) vulnerability. Due to insufficient validation of end-user supplied input, an authenticated, remote attacker can conduct an XSS attack 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 CVSS v3 base score for this vulnerability is 6.5 and the temporal score is 5.7 which results in this vulnerability being rated as MEDIUM.

## Determination of Exploitability

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

No known exploits are available for this vulnerability as indicated in <https://www.tenable.com/plugins/nessus/184369> for this vulnerability.

CVSS v3 Base score is 9.8 OR critical

The Attack Vector is network based, Attack Complexity is low, Privileges are not required and User Interaction is not required.

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

No known exploits are available for this vulnerability as indicated in <https://www.tenable.com/plugins/ot/501888> for this vulnerability.

CVSS v3 Base score is 7.2 OR High.

The Attack Vector is network based, Attack Complexity is low, Privileges are high and User Interaction is not required.

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

No known exploits are available for this vulnerability as indicated in <https://www.tenable.com/plugins/ot/502147> for this vulnerability.

CVSS v3 Base score is 6.5 OR Medium.

The Attack Vector is network based, Attack Complexity is low, Privileges are low and User Interaction is required.

## Impact Analysis

This seeks to assess the potential impact to the client organization if the vulnerability is exploited.

Evaluate the significance of the affected system to Power pulse operations.

Consider the type of data or processes that are at risk.

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

A total of 40 Desktops and laptops are installed with this software and thus contain client information on them. A successful exploitation of this vulnerability could lead to a major loss of sensitive data that could include client personal and financial information as well as company privileged information.

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

If an attacker could gain access to network configurations due to the flaw in configuration service of affected devices this vulnerability if successfully exploited could expose all 3 substations to issues affecting OT and disruptions in service.

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

An attacker can conduct a cross site scripting (XSS) attack against a user of the web 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 and browser-based information. This mostly compromises web-based applications and thus continuous access to daily routine via the web interface is at risk.

## 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 environment.

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

Consideration should be given to compensating controls that can mitigate risk. The CVSS 3.1 calculator has been 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)**](https://www.tenable.com/plugins/nessus/184369)

The network environment for Zoom's Windows Desktop Client and VDI Client involves a combination of LAN and WAN connections, utilizing Zoom's cloud-based infrastructure to facilitate communication and collaboration among users across different locations. With a total of 40 desktops and laptops affected, sensitive data stored in these systems are at risk.

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>

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

The 6 Siemens Remote Terminal Units (RTUs) are located at Power Pulse’s 3 distribution stations.

these stations are each protected by a firewall, so all traffic traveling to the station across Power Pulse’s wide area networks needs to pass through a firewall located at each station. Therefore, an attacker would need to get onto the local network to exploit devices located in the 3 stations and as such the modified attack vector can be set to adjacent as an attacker would need to connect to LAN to exploit this vulnerability.

The CVSS 3.1 calculator was used to calculate an environmental score for this vulnerability. The environmental severity of this vulnerability is 5.9 (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:H/IR:H/AR:H/MAV:A>

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

This vulnerability impacts 35 SIP phones (model 3905) that are all located at Power Pulse’s head office however these devices are considered of low importance from a confidentiality, integrity, and availability perspective, as they aren’t used that often.

The CVSS 3.1 calculator was used to calculate an environmental score for this vulnerability. The environmental severity of this vulnerability is 4.1 (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:L/E:U/RL:O/RC:C/CR:L/IR:L/AR:L>

## Threat Environment

In 2022, energy companies in North America suffered 20% of attacks, making energy the most attacked industry.

The type of attacks varied with 40% starting by cyber criminals exploiting public-facing applications. Spear phishing links and external remote services made up 20% of energy attacks. Other types of attacks included data theft (23%), extortion (23%), ransomware (15%), BEC (15%), credential harvesting (15%) and botnet infections (19%).

Among critical infrastructure sectors, the oil and gas industry in Canada witnessed the highest percentage of cyber incidents, with approximately a quarter of organizations reporting such occurrences. Power pulse, however has experienced no major security incidents in recent years, aside from encountering phishing emails that were effectively blocked by the corporate email security platform. Nevertheless, as highlighted in the National Cyber Threat Assessment of 2020, the level of interconnectedness within an organization directly correlates with the extent of its threat surface, potentially amplifying the range of cyber threats it may encounter.

It is recommended that Power pulse remains vigilant against the threat of potential attacks from range of threat actors.

## Prioritization.

|  |  |  |
| --- | --- | --- |
| **Vulnerability#** | **Recommended Implementation Timeframe** | **Rationale** |
| vulnerability #1> [**Zoom Client for Meetings < 5.15.2 Vulnerability (ZSB-23038)**](https://www.tenable.com/plugins/nessus/184369) | Should be remediated as soon as possible, within 24-48 hours. | With 40 desktops containing sensitive data being affected, there is a high risk of an unauthenticated user enabling an escalation of privilege via network access. |
| <vulnerability #2> [**Siemens (CVE-2023-42797)**](https://www.tenable.com/plugins/ot/501888) | Should be addressed within 14 days as they can pose a significant risk and can be exploited by threat actors. | As internet access from the 3 stations have been halted to minimize the risk of remote access, the ability to manipulate configurations is still significant. |
| <vulnerability #3> [**Cisco IP Phone Stored XSS (cisco-sa-uipphone-xss-NcmUykqA)**](https://www.tenable.com/plugins/nessus/186612) | Should be addressed within 30 days as they present a moderate risk and can potentially be exploited with other vulnerabilities. | 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. |

## Plan of Action

The most critical vulnerability assessed is the [Zoom Client for Meetings < 5.15.2 Vulnerability (ZSB-23038)](https://www.tenable.com/plugins/nessus/184369) an internet-facing software at power pulse utilities. This vulnerability could result in the exposure of both company and customer personal information and should be remediated as quickly as possible by upgrading the version of zoom installed to Zoom Client for Meetings 5.15.2 or later.

The next vulnerability that should be addressed is [Siemens (CVE-2023-42797)](https://www.tenable.com/plugins/ot/501888). The recommended course of action as per vendor advisory is to review the list of users that are allowed to modify the network configuration and apply strong passwords. Default account credentials should be changed and monitored periodically.

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

presents the lowest level of risk to Power pulse based on the nature of usage, nature of the vulnerability and potential impact if the vulnerability was exploited. The solution as per vendor advisory is to upgrade the software to a secure version having Cisco bug ID CSCwf58594 for the SIP Phone 3905 in the next 30 days.

## Conclusion

In conclusion, this vulnerability assessment has revealed a critical vulnerability, one high and a medium-priority vulnerability in Power pulse’s environment. These vulnerabilities, if left unchecked, could potentially lead to unauthorized access, data breaches, and other security incidents that could have impacts on Power pulse’s operations and reputation.

Key findings include an out-of-date system software on a remote host, a flaw/misconfigured access controls and a compromised web interface on Power pulse’s Environment.

Therefore, it is recommended that Power pulse remediate the vulnerabilities outlined in this report in line with the detail contained in the Prioritization and Plan of Action sections of this report. Power pulse’s proactive efforts in addressing these issues will play a vital role in safeguarding the organization against future cyber threats.