**The POWER PULSE UTILITIES**

# **Vulnerability assessment Report**

March 7th, 2024

Leonard Offor

## Executive Summary

This report presents findings from a vulnerability assessment conducted for Power Pulse Utilities on March 7th, 2024. The goal of this assessment report is to evaluate the security vulnerabilities identified within Power Pulse’s systems and network infrastructure. This report evaluates the vulnerabilities identified from both an exploitability and impact perspective and recommends potential mitigation strategies.

Key Insights:

● 3 vulnerabilities were identified across the IT and OT systems evaluated in the vulnerability scan.

● 1 vulnerability was classified as High, 1 other vulnerability was classified as Medium, and 1 was rated Low

● The most severe vulnerability, Zoom Client for Meetings <5.12.2, could allow unauthorized access to sensitive customer data and could also impact core business function of Power Pulse but there is no reported case of any exploit for this in the wild.

● A medium risk vulnerability was identified in 6 Siemens Remote Terminal Unit (RTU) that is active in all 3 substations of Power Pulse Utilities. There is no known exploit for this vulnerability in the wild and due to these devices being inside a firewall protected network that filters internet traffic out, an attacker would need local access to exploit the vulnerability.

● A low risk vulnerability was identified on the 35 SIP phones from Cisco. These devices are not often in use and there is no exploit found in the wild for this vulnerability. There is a low impact to Confidentiality, Availability and Integrity for this vulnerability in the context of Power Pulse Utilities environment.

● Systems with missing patches account for 100% of the vulnerabilities identified and one of them also has a work around recommended by the manufacturer.

## Introduction

Purpose:

The purpose of this exercise is to perform a detailed vulnerability assessment of the entire information technology infrastructure of Power Pulse Utilities in order to rank them according to order of prioritization for remediation.

Scope:

The target scope of this activity includes all Information technology (IT) & Operational Technology (OT) assets that are on the network of Power Pulse Utilities.

## Identification of Vulnerabilities

The results from the recent vulnerability scan shows the three vulnerabilities listed below

* Vulnerability #1 – Zoom Client for Meetings <5.15.2 Vulnerability (ZSB-23038) (CVE-2023-39213)
* Vulnerability #2 – Siemens (CVE-2023-42797)
* Vulnerability #3 – CISCO IP Phone Stored XSS (CVE-2023-20265)

## Analysis Using Vulnerability Databases

A detailed analysis into the identified vulnerabilities on external sources such as the NIST’s NVD (National Vulnerabilities Database), FIRST’s CVSS (Common Vulnerability Scoring System) & Vendor webpages related to these vulnerabilities was carried out and the following information was discovered for each vulnerability:

* Vulnerability #1 – Zoom Client for Meetings <5.15.2 Vulnerability (ZSB-23038) ([CVE-2023-39213](https://nvd.nist.gov/vuln/detail/CVE-2023-39213))
* This is a vulnerability that affects the software Zoom desktop client for Windows and Zoom VDI client before version 5.15.2. The vendor responsible for this software is Zoom Video Communications inc.
* Improper neutralization of special elements in output used by a downstream component in the vulnerable software is the cause of vulnerability. ([CWE-74](https://cwe.mitre.org/data/definitions/74.html))
* The vulnerability can allow an unauthenticated user to enable an escalation of privilege via network access.
* This vulnerability has a CVSSv3.1 base score of 9.8 or Critical as at the time of compiling this report.
* Zoom advised users to keep themselves secure by applying current updates or downloading the latest zoom software with all current security updates from <https://zoom.us/download>
* Vulnerability #2 – Siemens ([CVE-2023-42797](https://nvd.nist.gov/vuln/detail/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.
* 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.
* The SICAM A8000 RTUs (Remote Terminal Units) series is a modular device range for telecontrol and automation applications in all areas of energy supply.
* This vulnerability has a CVSSv3.1 base score of 7.2 or High as at the time of compiling this report
* Siemens has released new versions for the affected products and recommends to update to the latest versions.
* Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:
* Review the list of users that are allowed to modify the network configuration and apply strong passwords.
* General security recommendations which can be found at [https://www.siemens.com/grid-security](https://www.siemens.com/global/en/products/energy/energy-automation-and-smart-grid/grid-security.html)
* Vulnerability #3 – CISCO IP Phone Stored XSS ([CVE-2023-20265](https://nvd.nist.gov/vuln/detail/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.
* 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.
* This vulnerability has a CVSSv3.1 score of 5.4 or Medium as at the time of compiling this report.
* Cisco has released the list of vulnerable Cisco products as well as software updates that address this vulnerability which can be found in the official [advisory](https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-uipphone-xss-NcmUykqA). There are no workarounds that address this vulnerability.

## Determination of Exploitability

Further investigation was conducted to determine the exploitability of the vulnerabilities discovered in Power Pulse’s network and the following are the finding made;

* Zoom Client for Meetings <5.15.2 Vulnerability (ZSB-23038) (CVE-2023-39213):
  + No known exploits are available for this vulnerability based on [tenable plugin](https://www.tenable.com/plugins/nessus/184369)
  + The CVSSv3 base score for this vulnerability is 9.8 or Critical
  + The breakdown of the exploitability metrics are as follows:
    - Attack Vector: Network
    - Attack Complexity: Low
    - Privileges are not required.
    - User Interaction is not required
* Siemens (CVE-2023-42797)
  + No known exploits are available for this vulnerability based on [tenable plugin](https://www.tenable.com/plugins/ot/501888)
  + The CVSSv3 base score for this vulnerability is 7.2 or High
  + The breakdown of the exploitability metrics are as follows:
    - Attack Vector: Network
    - Attack Complexity: Low
    - Privileges required: High
    - User Interaction is not required
* CISCO IP Phone Stored XSS (CVE-2023-20265)
  + No known exploits are available for this vulnerability based on [tenable plugin](https://www.tenable.com/plugins/nessus/186612)
  + The CVSSv3 base score for this vulnerability is 5.4 or Medium
  + The breakdown of the exploitability metrics are as follows:
    - Attack Vector: Network
    - Attack Complexity: Low
    - Privileges required: Low
    - User Interaction is required

## Impact Analysis

In this section we dive a little deeper into these vulnerabilities to assess the impact as it relates to Power Pulse network & systems.

* Vulnerability #1 - Zoom Client for Meetings <5.15.2 Vulnerability (ZSB-23038) (CVE-2023-39213): Zoom client is used for hosting video meeting is vital for Power Pulse Utilities employees to be able to effectively collaborate with both internal and external stakeholders. 40 windows desktop and laptops have the vulnerable Zoom client software installed on them. If successfully exploited a remote unauthenticated attacker can have admin privileges on these machines and can use that to exploit the entire organization’s network. Also, these laptops contain confidential client information which Power pulse is bound by obligation to compliance with the energy regulatory framework to protect from unauthorized access. If such information were to be exfiltrated by the attacker, it would damage Power pulse’s reputation and attract financial punishments against the organization.
* Vulnerability #2 – Siemens SICAM A8000 CP command Injection (CVE-2023-42797): The vulnerable component in Power pulse environment are 6 Siemens Remote Terminal Units (RTUs) that are located in Power pulse’s 3 distribution stations. RTUs are mobile devices for telecontrol and automation in all areas of energy supply. If these vulnerabilities are successfully exploited a remote attacker can inject commands that will be executed on the local device using root privileges. This can be leveraged to cause power outages or other aims of the attacker. However, the attacker would need to get onto the network to exploit any devices in the substation. These stations are isolated by a firewall, which checks every traffic coming from outside the network and applies strict rules to allow only safe connections through to the local network. All connections from the internet are currently being configured to not be allowed on the substation firewalls.
* Vulnerability #3 – Cisco IP Phone Stored XSS (CVE-2023-20265): The Cisco IP phone vulnerability on the scan report affects 35 SIP phones (model 3905) that are located at the Power Pulse’s head office. This vulnerability uses a cross site scripting attack technique that requires a user to interact with the payload in order for the exploit to be successful. However, these phones aren’t used as often since most employees use their corporate cell phones or Zoom client on their computers to call colleagues and all calls from clients are routed to a separate call center operated by a 3rd party organization.

## Contextualization

To effectively determine the risk these vulnerabilities pose to Power Pulse utilities, in this section we would analyze each vulnerability in the context of the environment in which it was found to determine the impact if it were to be exploited by a threat actor.

We make use of the Environment metrics from CVSS v3.1 calculator by FIRST to customize the severity score of the vulnerabilities we found based on Power Pulse’s environment by modifying the Base and Temporal scores based on the unique characteristics of Power Pulse’s systems & networks. This exercise will give us a better understanding of the overall risk landscape and how to deploy limited resources towards their mitigation.

**Vulnerability #1 - Zoom Client for Meetings <5.15.2 Vulnerability (ZSB-23038) (CVE-2023-39213):** The zoom client affected by this vulnerability makes use of Internet protocol for communication which increases it’s attack surface. Also, the confidential nature of data that is stored in the laptops that have vulnerable zoom client software resulted in a high scoring for the confidentiality, availability & integrity metrics of this vulnerability. Zoom has released updates that will patch these systems and thus we have a calculated Environmental score of 8.5 or 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](https://www.first.org/cvss/calculator/3.1%23CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C)

Vulnerability #2 – Siemens SICAM A8000 CP command Injection (CVE-2023-42797): The 6 RTUs that have this vulnerable firmware from Cisco are all in isolated networks that are in a perimeter by firewall which excludes all internet traffic from accessing the networks. So an attacker would have to be in the local network to be able to exploit this vulnerability. Based on that we change the Modified Attack Vector (MAV) to ‘Local’ and that gives a calculated Environment Score of 5.8 or 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/MAV:L](https://www.first.org/cvss/calculator/3.1%23CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C/MAV:L)

Vulnerability #3 – Cisco IP Phone Stored XSS (CVE-2023-20265): The 35 Cisco SIP phones in the Power Pulse head office that have this vulnerability are not often used by employees who instead use Zoom client and their corporate phones routed to a 3rd party network for making calls. This results in a low requirement for confidentiality, integrity & availability in the Environment scoring. There we have an environment score of 3.5 or Low for this vulnerability.

[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](https://www.first.org/cvss/calculator/3.1%23CVSS: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

In the past 25years OT has adopted data and processing and communication protocols from IT to create safer, smarter and more efficient operations. The global market for smart OT devices in 2019 was estimated to be about $205.5 billion CAD, growing at 8% per year. Many Canadian organizations are adopting this global trend. We judge that a significant proportion of Canada’s OT is becoming accessible from the internet and other untrusted networks and that this will almost certainly increasingly expose these OT systems to cyber threats.

In March 2021, roughly 128,000 network ports associated with OT services responded to scans from Shodan (a search engine for Internet-connected devices) from about 62,800 unique internet protocol (IP) addresses that geolocated to Canada. About 13% of those IP addresses advertised a software version with at least one publicly-reported vulnerability from the Common Vulnerabilities and Exposures (CVE) list—a reliable, but not absolute indicator of vulnerability. We assess that this likely represents a range of Canada-based industrial OT devices that are accessible via the Internet, including equipment typically used by highly-automated CI sectors, and that a small but significant proportion of these devices are likely exploitable through known vulnerabilities ([Shodan Scan Results](https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-threat-operational-technology#fn*)). The IP addresses geolocated to every province and territory, with the highest concentrations in Ontario and Quebec.

Cyber threat actors have a choice of several routes through which to direct cyber threat activity against OT – Direct or Indirect targeting. The cyber threat to OT from direct targeting derives from two main sources: financially motivated, medium-sophistication cybercrime groups, and politically-motivated, high-sophistication state-sponsored cyber threat actors. Other potential actors, such as terrorists, hacktivists, and thrill seekers tend to be low-sophistication and present a much lower threat. From 2010 to 2019, there were on average about 2 significant incidents per year, but in 2020, that number increased to 8. We assess that the 2020 spike in cyber activity that affected OT was almost certainly due to an increase in criminal actor activity against large industry, where the OT effect was a by-product of targeting IT networks, as well as OT targeting by states.

IAM synchronization between IT and OT networks (for ease of administration) is an emerging OT vulnerability. Cyber actors are learning to exploit IAM servers to facilitate lateral movement in a network. Synchronizing or mirroring the IAM service into an otherwise protected OT network gives these actors access to vulnerable OT assets. An incident using this method was reportedly the cause of a US pipeline shutdown from ransomware in 2019.

Finally, the cyber threat landscape experienced by the OT asset operators in Canada is evolving, and cyber threat actors continue to adapt their activities to try to stay ahead of defenders. We identify trends within the OT threat landscape, including the growing threat from cybercriminals, the threat from state-sponsored actors, as well as the introduction of new threat vectors stemming from the adoption of new technology and Internet-connected devices. As noted in the National Cyber Threat Assessment 2020, many cyber threats can be mitigated through awareness and best practices in cyber security and business continuity. Cyber threats continue to succeed today because they exploit deeply-rooted human behaviours and social patterns, and not merely technological vulnerabilities. Defending Canada against cyber threats and related influence operations requires addressing both the technical and social elements of cyber threat activity. Cyber security investments will allow Canadians to benefit from new technologies while ensuring that we do not unduly risk our safety, privacy, economic prosperity, and national security.

## 

## Prioritization.

|  |  |  |
| --- | --- | --- |
| **Vulnerability#** | **Recommended Implementation Timeframe** | **Rationale** |
| #1 – Zoom Client for Meetings <5.15.2 Vulnerability (ZSB-23038) (CVE-2023-39213) | Within 14 days | Internet facing systems which store sensitive confidential client data and can cause significant damage if exploited however there is no proven exploits in the wild for it. |
| #2 – Siemens SICAM A8000 CP command Injection (CVE-2023-42797): | Within 30 days | RTU devices vulnerable to remote code injection but only if exploited from within the local network due to internet traffic filtering firewall on perimeter. |
| #3 – Cisco IP Phone Stored XSS (CVE-2023-20265): | Within 90 days | Vulnerable Cisco SIP phones not frequently in use and have low impact to confidentiality, integrity & availability in Power Pulse Utilities environment |

## Plan of Action

The most crucial vulnerability in order of priority to remediate is the Zoom Client for Meetings <5.15.2 Vulnerability which was found on 40 IT assets that is exposed to the internet. Despite the fact that there is no known exploit in the wild for this vulnerability, if exploited by a malicious actor, could lead to exposure of sensitive confident client data and should be remediated within 14days of the publishing of this report by downloading the latest and secure version of the Zoom client software which is 5.15.2 and above.

The next vulnerability that needs to be addressed on the Power Pulse Utilities network is Siemens SICAM A8000 CP command Injection vulnerability which impacts all 3 substations of the organization. While there have been no report incidents of exploits for this vulnerability and the fact that it would only require local network access to exploit this vulnerability, an attacker could successfully inject and execute commands remotely leveraging on this vulnerability so it should be remediated within 30 days of publishing this report by downloading and applying firmware updates from Siemens for these units. Also, special attention needs to be given to strengthen physical as well as network security and restrict unauthorized access to the local network. Finally, appropriate resilience measures need to be incorporated into the grid design and ensure that the substation networks are strongly segmented with VPN and/or firewalls in place.

Lastly, the Cisco IP Phone Stored XSS vulnerability found on the 35 SIP phones from Cisco at the Head Office needs to be patched using the latest released software update from Cisco within 90 days of the publishing of this report. The minimal risk to Confidentiality, Integrity & Availability to Power Pulse utilities due to infrequent use of these devices and available of safer phone call alternative technologies ensure that there is less risk associated with this vulnerability until resources are available to apply the remediation plan recommended in this report.

## Conclusion

In conclusion, this vulnerability assessment has revealed a critical vulnerability, one medium and also one low vulnerability in Power Pulse Utilities’ environment. These vulnerabilities, if left unchecked could potentially lead to unauthorized access, data breaches, remote code execution and denial of service incidents that could impact on Power Pulse Utilities’ operations and damage its reputation.

Key findings include a flaw in the Zoom Client software for hosting meetings in Power Pulse Utilities’ environment, vulnerable OT hardware in 3 substation lab and vulnerable Cisco IP telephones firmware that can be exploited to perform a cross site scripting attack. It is recommended that Power Pulse Utilities remediate the vulnerabilities outlined in this report in line with the details contained in the Prioritization and Plan of Action sections of this report.

Power Pulse Utilities also needs to adopt a proactive approach in threat mitigation by constantly assessing its threat environment and leveraging several threat intelligent sources and communities within the energy industry. Modern tools for monitoring direct and indirect threats need to be deployed and a robust incident response plan need to be developed to successfully navigate future attacks on the network.