The POWER PULSE UTILITIES

Vulnerability Assessment Report

August 4, 2024

Prepared by: Aurnob Jahin Islam

Executive Summary

This report presents findings from a vulnerability assessment of a scan that was conducted in January 2024 by a third-party security consultation company. 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 Power Pulse 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 vulnerability scan report.
- A critical rated vulnerability was identified for Zoom Client for Meeting application installed on 40 Windows systems used by the employees of Power Pulse Utilities.
- A high rated vulnerability was identified in Siemens Remote Terminal Units which are spread across 3 distribution stations within the infrastructure of Super Pulse Utilities.
- A medium rated vulnerability was found within the Cisco IP based telephones that are used in the head office of Super Pulse Utilities.

Critical	High	Medium	Low
1	1	1	0

This report presents an analysis of the current security vulnerabilities identified across Power Pulse Utilities' Information Technology (IT) and Operation Technology (OT) environments. The vulnerabilities identified in the scan report have been further assessed considering the compensating controls in Power Pulse's environment and the potential impacts if the 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

This report presents a thorough analysis of the current security vulnerabilities identified withing Power Pulse Utilities' IT and OT infrastructure. The focus of this assessment and report is to identify risks that could be exploited by attackers and provide recommendations to improve the organization's security posture.

Purpose:

- Identify vulnerabilities in networked systems, applications, and infrastructure.
- Evaluate the potential impact of discovered vulnerabilities to business operations.
- Provide proper implementation recommendations to mitigate risk associated with each vulnerability.

Scope:

- The vulnerability assessment covered systems, infrastructure, and application in Power Pulse Utilities' Operational Technology (OT) and Information Technology (IT) environments.

Identification of Vulnerabilities

The Power Pulse Utilities provided the results from a recent vulnerability scan that was completed by a third-party consulting company they hired. The consulting company used a commercial vulnerability scanning tool to conduct the scanning and it found the following vulnerabilities.

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

Vulnerability #2: Siemens SICAM A8000 CP Command Injection (CVE-2023-42797)

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

Analysis Using Vulnerability Databases

Vulnerability #1 – Zoom Client for Meeting < 5.15.2 Vulnerability (ZSB-23038)

As per Tenable – (ZSB-23038) and Zoom's security bulletin, the version of Zoom Client for Meetings installed on the remote host 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 version 5.15.2 may allow an unauthenticated user to enable an escalation of privilege via network access.

This security flaw could potentially allow an attacker to exploit the systems, leading to unauthorized as well as escalated privilege access, which allows room for execution of arbitrary code.

This vulnerability is rated Critical for its severity as its CVSS v3 Base Score is 9.8 and Temporal Score is 8.5.

Vulnerability #2 – Siemens SICAM A8000 CP Command Injection (CVE-2023-42797)

As per (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 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 (CVE-2023-20265)

As per Nessus Plugin ID 186612, 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 vulnerability in the web-based management interface of a small subset of this IP based telephony could allow an authenticated, remote attacker to conduct a stored XSS attack against a user of the interface on an affected device. Based on Cisco's security advisory, attacker must have valid credentials to access this web-based management interface of the affected device in order to exploit this vulnerability.

The CVSS v3 risk factor rating for this vulnerability is Medium as its base score is 5.4 and temporal score is 4.7.

Determination of Exploitability

- Vulnerability #1 – Zoom Client for Meeting < 5.15.2 Vulnerability (ZSB-23038)
  - Currently there is no known exploit for this vulnerability as per Tenable's plug-in entry.
  - 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 – Siemens SICAM A8000 CP Command Injection (CVE-2023-42797)
  - Exploits are not available currently for this vulnerability as per Tenable's plug-in entry.
  - The CVSS v3 Base score is 7.2 or High.
  - The Attack Vector is network based, the Attack Complexity is Low, Privileges are required as it is rated High and User Interaction is Not Required.
- Vulnerability #3 – Cisco IP Phone Stored XSS (CVE-2023-20265)
  - Exploits are note available currently for this vulnerability as per Tenable's plug-in entry.
  - The CVSS v3 Base score is 5.4 or Medium.
  - The Attack Vector is Network based, the Attack Complexity is Low, some Privileges are required as it is rated Low and User Interaction is Required.

Impact Analysis

This is the impact of the three vulnerabilities that were found after conducting the vulnerability scan:

Vulnerability #1 – Zoom Client for Meeting < 5.15.2 Vulnerability (ZSB-23038):

Since the 40 Windows host machines used by Power Pulse's employees are installed with the Zoom Client application to conduct meetings with clients and which also store client information, their information is at a high risk of being compromised.

Vulnerability #2 – Siemens SICAM A8000 CP Command Injection (CVE-2023-42797):

There are 6 Siemens Remote Terminal Units (RTUs) which posses this vulnerability. These machines are in the 3 distribution stations of Power Pulse and internet access is not available from the stations' networks. Therefore, an attacker would need to get onto the local network to exploit these devices located in the 3 stations. In addition, there are firewalls located behind each of these stations. If compromised and attacker escalates privilege, attacker can inject commands and retrieve information. Due to the nature of these devices and how they are placed within the infrastructure, the risk is high if they get compromised.

Vulnerability #3 – Cisco IP Phone Stored XSS (CVE-2023-20265):

There are 35 SIP phones located at the head office of Power Pulse. These devices are of low importance as other means such as corporate cell phones or Zoom applications are used for communication instead of SIP phones. Even if there was a compromised SIP device, the impact would be low.

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 form a business process perspective.

Consideration should be given to compensating controls that can mitigate risk. The CVSS v3.1 calculator has been used to determine an adjusted score for each vulnerability based on the Environmental Scores.

Vulnerability #1 – Zoom Client for Meeting < 5.15.2 Vulnerability (ZSB-23038):

The Zoom application installed on the Windows machines used by the Power Pulse's employees are affected by this vulnerability. These machines contain sensitive information about Power Pulse's operations and contain confidential client information. Integrity and availability are also important for this application as it is highly used for communication with clients. This vulnerability is urgent in nature to have a secure path of communication with clients.

The CVSS v3.1 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/3.0#CVSS:3.0/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 SICAM A8000 CP Command Injection (CVE-2023-42797):

The Siemens RTUs are affected by this vulnerability and these RTUs are located in 3 distribution stations within Power Pulse's infrastructure. Although there is no internet access from the station networks and there are firewalls installed at each station, these devices could still be exploited if an attacker gains local network access. The Confidentiality, Integrity, and Availability for the environment of this vulnerability is high, the Attack Vector environment is Local and High Privilege is Required.

The CVSS v3.1 calculator was used to calculate an environmental score for this vulnerability. The environmental severity of this vulnerability is 5.8 (medium).

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/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:L/MPR:H

Vulnerability #3 – Cisco IP Phone Stored XSS (CVE-2023-20265):

These Cisco phones are affected by this vulnerability. These Cisco IP telephones are in Power Pulse's main head office and are not used often as there are alternatives. The Confidentiality, Integrity and Availability are considered low in terms of importance. In addition, user interaction is required to exploit this vulnerability.

The CVSS v3.1 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/3.0#CVSS:3.0/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/MUI:R/MS:C/MA:N

Threat Environment

The energy sector, especially oil and gas organizations based on The cyber threat to Canada's oil and gas sector report showcases the broad attack surface which is connected to digital systems within these energy sectors. According to the report, Statistics Canada survey data shows 25% of Canadian energy sector organizations have experienced cyber incidents in 2019 alone.

Based on the report, threat actors target these organizations by targeting its supply chain which serves two purposes. First purpose is to obtain commercially valuable intellectual property and to infiltrate supplier. Secondly, to obtain target organization's network and OT (Operational Technology) information and exploit the indirect route from supplier to target organization. To support this argument even further, based on the World Economic Forum's article on cyber incidents against

energy sector, cyber attackers first infiltrate suppliers to move laterally into an energy organization's network. This report also indicates a key statistic surveyed and determined by SANS that 59% of cybersecurity teams identified technical integration of legacy OT and modern IT systems to be the biggest challenge to securing OT.

Parallel transformations of other sectors such as manufacturing, technology and automotive are also in this chain of threat as these sectors are all dependent on energy sector, based on this latest report published by KPMG. With the increased attack surfaces due to a variety of threat vectors, experts suggest modernizing supply chain security and align cybersecurity with each organization's resilience.

Prioritization

Vulnerability#	Recommended Implementation Timeframe	Rationale
#1 – Zoom Client for Meeting < 5.15.2 Vulnerability (ZSB-23038)	24-48 hours	This can allow unauthorized access or remote code execution if exploited. This could result in exfiltration of sensitive data. Thus, this vulnerability is labelled as critical.
#2 – Siemens SICAM A8000 CP Command Injection (CVE-2023-42797)	14 days	Although, these devices are behind a firewall and require privilege escalation for access, the level of risk is high as an exploitation to this vulnerability could lead attacker to move laterally within the network.
#3 – Cisco IP Phone Stored XSS (CVE-2023-20265)	30 days	Exposed systems to this vulnerability are not often used. Thus, it is rated as medium and should be treated as such to avoid any exploitation.

Plan of Action

The critical rated vulnerability that was found in the vulnerability scan report from the third-party company is the Zoom Client for Meeting for using a version older than 5.15.2. This vulnerability, if exploited, can result in exposure to confidential information about Power Pulse's operation and client information. The remediation to this vulnerability is to upgrade to Zoom Client version 5.15.2 or later as quickly as possible.

The next vulnerability that should be addressed is the Siemens RTUs command injection flaw which is rated as high in the third-party provided vulnerability scan report. These devices are internal devices sitting behind firewalls in 3 geo-separated distribution stations. If not remediated, it could potentially disrupt operations and lead to unauthorized control over the device. It is advised to implement vendor applied patches as soon as they are released for the RTUs.

The medium rated vulnerability in the vulnerability scan report is related to stored cross-site scripting for Cisco IP Phones. This vulnerability requires user interaction to execute the script to exploit the systems. The remediation for this vulnerability is vendor specific. It is advised to refer to Cisco bug IDs CSCwf58592 and CSCwf58594 to remediate this vulnerability.

Conclusion

This vulnerability assessment has disclosed one critical vulnerability, one high vulnerability and one low vulnerability within the environment of Power Pulse Utilities. Although there is no exploit available for these vulnerabilities, but if they are not remediated, they could potentially lead to unauthorized

access, information disclosure and other security incidents that could have an impact on Power Pulse Utilities' operations.

The critical vulnerability discovered is affecting the Zoom Client application installed on Windows desktops or laptops. This vulnerability should be remediated by updating the application withing the next 24-48 hours. The high vulnerability discovered is affecting the Siemens Remote Terminal Units in Power Pulse Utilities' distribution stations. The medium vulnerability discovered is affecting the Cisco IP Phones located in the head office of Power Pulse Utilities. Both vulnerabilities should be remediated using the vendor provided patches accordingly and should be patched on schedule.

Proactive manner should be considered to remediate these vulnerabilities based on the Prioritization and Plan of Action sections outlined in this report. Proper action against these vulnerabilities would result in a stronger cyber defense to safeguard the operations and data of Super Pulse Utilities.