The POWER PULSE UTILITIES

Vulnerability Assessment Report

May 26, 2024
Prepared By: Angel Mary George

Executive Summary

This report presents the results of a vulnerability assessment conducted for Power Plus Utilities, aimed at evaluating security weaknesses within the organization's systems and network infrastructure. It provides an analysis of identified vulnerabilities from both exploitability and impact perspectives, along with recommendations for potential mitigation strategies.

Key Insights:

- The vulnerability scan revealed three vulnerabilities across both IT and OT systems.
- Among these, one vulnerability was classified as Critical, one as High, and one as Medium severity.
- The most critical vulnerability, CVE-2023-39213, poses a significant risk by potentially allowing unauthorized users to exploit network access, leading to a possible escalation of privileges.
- A notable observation is that 75% of identified vulnerabilities are attributed to systems lacking necessary patches.

Introduction

This report represents an analysis of the current security vulnerabilities identified within Power Plus Utilities's IT and OT infrastructure. The focus of this assessment and in turn this report is identifying risks that could be exploited by attackers and providing 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 actionable recommendations to mitigate risk associated with vulnerabilities.

Scope

- The assessment covered systems, infrastructure and applications in Power Plus Utilities's Operational Technology (OT) and Information Technology (IT) environments.

Identification of Vulnerabilities

Power Pulse Utilities has provided the recent results from a vulnerability scan conducted by a third-party vendor utilizing a commercial vulnerability scanning platform.

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 including, Tenable's Vulnerability Plug-In Database, NIST's National Vulnerability Database and CISA's Cybersecurity Alerts & Advisories site.

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

As per CVE-2023-39213,The Zoom Client for Meetings installed on the remote host is vulnerable due to the version being prior to 5.15.2. This vulnerability is detailed in the ZSB-23038 advisory, indicating that improper neutralization of special elements exists in Zoom Desktop Client for Windows and Zoom VDI Client versions before 5.15.2. This security flaw may allow an unauthenticated user to exploit the network access, potentially enabling an escalation of privilege.

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)

CVE-2023-42797 outlines that a vulnerability has been discovered in the CP-8031 MASTER MODULE and CP-8050 MASTER MODULE, affecting all versions prior to CPCI85 V05.20. The issue lies within the network configuration service of these devices, where a flaw in the conversion of IPv4 addresses could lead to the use of an uninitialized variable in subsequent validation steps. This vulnerability can be exploited by an authenticated remote attacker through the upload of a specially crafted network configuration. This could potentially allow the attacker to inject commands that are executed with root privileges during the device's startup, posing significant security risks.

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)

As per CVE-2023-20265 , this vulnerability has been identified in the web-based management interface of certain Cisco IP Phones, which could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This issue stems from insufficient validation of user-supplied input. An attacker could exploit this vulnerability by persuading a user to view a page containing malicious HTML or script content. Successful exploitation could enable the attacker to execute arbitrary script code within the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker must possess valid credentials to access the web-based management interface of the affected device.

CVSS v3 base score for this vulnerability is 5.4 and the temporal score is 4.7 which results in this vulnerability being rated as Medium.

Determination of Exploitability

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

No known exploits are available for this vulnerability as indicated in Tenable's plugin entry for this vulnerability.

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

No known exploits are available for this vulnerability as indicated in Tenable's plugin entry for this vulnerability.

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

No exploits are available currently for this vulnerability as indicated in Tenable's plugin entry for this vulnerability.

Impact Analysis

Assess the potential impact to the client organization if the vulnerability is exploited.
Evaluate the significance of the affected system to Power Pulse's operations.
Consider the type of data or processes that are at risk.

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

The identified vulnerability in the Zoom Client for Meetings installed on all 40 Windows desktops and laptops used by Power Pulse employees poses significant risks. These devices contain confidential information about the company's operations and potentially sensitive client data. Exploiting this vulnerability could lead to unauthorized access and a possibility of escalated privilege, resulting in data breaches that expose critical business and client information. The potential impacts include financial losses from incident response and regulatory fines, operational disruptions, and substantial reputational damage.

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

The vulnerability affecting the six Siemens Remote Terminal Units (RTUs) located at Power Pulse's three distribution stations poses substantial security risks, despite the protective firewalls at each station. Since an attacker must gain local network access to exploit the RTUs, the primary concern is the internal threat. This includes the potential for malicious insiders or compromised devices within the local network to bypass firewall protections. If exploited, the vulnerability could disrupt the critical functions of the distribution stations, leading to operational inefficiencies, power outages, and compromised system integrity.

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

The identified Cisco vulnerability impacts 35 SIP phones (model 3905) located at Power Pulse's head office. However, these devices are considered of low importance from a confidentiality, integrity, and availability perspective. The reason for this is that they are infrequently used, as most employees prefer using their corporate cell phones or the Zoom client on their computers for communication. Additionally, all client calls are routed through a separate call center managed by a third-party organization, further reducing the criticality of these SIP phones. Therefore, while the vulnerability exists, its potential impact on Power Pulse's operations is minimal due to the limited use and low reliance on these devices for essential communication functions.

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)

The identified vulnerability in the Zoom Client for Meetings, installed on all 40 Windows desktops and laptops used by Power Pulse Utilities employees, poses significant risks. These devices hold confidential information regarding the company's operations and potentially sensitive client data. If exploited, this vulnerability could lead to unauthorized access and a possibility of privilege escalation, resulting in data breaches that expose critical business and client information.

The CVSS 3.0 calculator was used to calculate an environmental score for this vulnerability.The overall 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 (CVE-2023-42797)

The vulnerability impacting the six Siemens Remote Terminal Units (RTUs) at Power Pulse Utilities's three distribution stations poses substantial security risks, even with the protective firewalls in place. Since an attacker needs local network access to exploit the RTUs, the primary concern is the internal threat.

The CVSS 3.0 calculator was used to calculate an environmental score for this vulnerability.The overall severity of this vulnerability is 5.9(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:A

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

The identified Cisco vulnerability affects 35 SIP phones (model 3905) located at Power Pulse Utilities's head office. However, these devices are considered to have low importance regarding confidentiality, integrity, and availability.

The CVSS 3.0 calculator was used to calculate an environmental score for this vulnerability.The overall severity of this vulnerability is 4.1(Medium) 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:L/E:U/RL:O/RC:C/CR:L/IR:L/AR:L

Threat Environment

In 2022, energy companies in North America were the most targeted industry, experiencing 20% of all cyberattacks. These attacks varied, with 40% originating from cybercriminals exploiting public-facing applications. Spear phishing links and external remote services accounted for 20% of these attacks. Other attack

types included data theft (23%), extortion (23%), ransomware (15%), business email compromise (BEC) (15%), credential harvesting (15%), and botnet infections (19%).

Following Russia's invasion of Ukraine, concerns about cyberattacks on the energy grid, particularly from the Killnet group, have intensified. The energy sector is a prime target for Killnet's distributed denial of service (DDoS) threats.

Given the rise in attacks against the North American energy sector in recent years, it is important to remain vigilant against potential threats from high-profile threat actors.

Prioritization.

Vulnerability#	Recommended Implementation Timeframe	Rationale
#1 - Zoom Client for Meetings < 5.15.2 Vulnerability (ZSB-23038)	24-48 hours	Zoom Client is installed on all 40 Windows desktops and laptops used by Power Pulse Utilities employees, poses significant risks.If exploited, this could lead to unauthorized access and a possibility of privilege escalation, resulting in exposing critical business and client information.
#2 - Siemens (CVE-2023-42797)	14 days	6 Siemens RTUs at Power Pulse Utilities's three distribution stations poses substantial security risks.Even though it's protected by a firewall, it can lead to the disruption of critical functions of the distribution stations if the vulnerability is exploited. Hence it should treat as High.
#3 - Cisco IP Phone Stored XSS (cisco-sa-uipphone-xss-NcmUykqA)	90 days	Even though 35 SIP phones (model 3905) located at Power Pulse Utilities's head office is at risk, because of low maintenance and infrequent usage it can be treated as Low .

Plan of Action

The most critical vulnerability identified in the Power Pulse Utilities organization during the assessment is the ZSB-23038 vulnerability in the Zoom Client, installed on all 40 Windows desktops and laptops used by Power

Pulse Utilities employees. These devices contain confidential information about the company's operations and potentially sensitive client data. Exploiting this vulnerability could lead to unauthorized access and control, resulting in the exposure of critical business and client information. Therefore, it is imperative to upgrade the Zoom Client to version 5.15.2 or later as quickly as possible.

The next vulnerability to address is the Siemens SICAM A8000 CP Command Injection, which affects six Siemens Remote Terminal Units (RTUs) at Power Pulse Utilities's three distribution stations. Despite the protection of a firewall and the requirement for an attacker to have local network access for exploitation, the primary concern remains the internal threat. It is recommended to update the module to CPCI85 V05.20 or later.

The vulnerability identified in Cisco IP Phone Stored XSS (cisco-sa-uipphone-xss-NcmUykqA) is classified as having the lowest priority due to its minimal maintenance requirements and infrequent usage. It is strongly advised to upgrade to the appropriate patched version mentioned in Cisco bug IDs CSCwf58592 and CSCwf58594 within a 90-day period.

Conclusion

In summary, this assessment uncovers vulnerabilities of varying severity within the Power Plus Utilities environment. These vulnerabilities pose risks ranging from critical to low priority, and if left unaddressed, could result in unauthorized access, data breaches, and other security incidents, potentially impacting Power Plus Utilities's operations and reputation.

Key findings include a critical vulnerability within the Zoom client installed on all Windows desktops and laptops used by Power Plus employees, a high vulnerability in six Siemens RTUs across Power Plus's three distribution stations, and a low vulnerability in Cisco IP Phone.

It is strongly recommended that Power Plus take action to remediate the vulnerabilities outlined in this report, following the prioritization and action plan detailed within. Proactive measures taken by the organization to address these issues will be crucial in fortifying against future cyber threats.