**The POWER PULSE UTILITIES** 

# **[Vulnerability Assessment Report]**

[2024-04-08]

[Rishabh Gautam]

## Executive Summary

A security checkup was done for Power Plus Utilities on April 8th, 2024. This checkup looked for weaknesses in the company's computer systems and network. The report details these weaknesses and how likely they are to be exploited by attackers. It also provides recommendations on how to fix these weaknesses and make the systems more secure.

|  |  |  |  |
| --- | --- | --- | --- |
| Critical | High | Medium | Low |
| [**Zoom Client for Meetings < 5.15.2 Vulnerability (ZSB-23038)**](https://www.tenable.com/plugins/nessus/184369) | [**Siemens (CVE-2023-42797)**](https://www.tenable.com/plugins/ot/501888) | [**Cisco IP Phone Stored XSS (cisco-sa-uipphone-xss-NcmUykqA)**](https://www.tenable.com/plugins/nessus/186612) |  |

Key Insights:

* 3 Vulnerabilities were identified across the Information and Online/Operational Transmission system during vulnerability scan.
* Zoom Client Meeting Vulnerability was considered a critical vulnerability whereas Siemens vulnerability was classified High and Cisco IP phone stored XSS vulnerability was medium.
* The system had an authentication bypass that needed to be fixed via patches which comprise 60% of the vulnerability

The report provides a thorough examination of the current security weaknesses found in Power Pulse Utilities' IT and online / operational transmission systems. It aims to pinpoint the most vulnerable risks that attackers could exploit and offers suggestions to enhance the organization's security measures.  
  
Purpose

* Identify key weakness in connected systems, application, and infrastructures.
* Assess the potential vulnerabilities that could affect business activities.
* Provide real life solutions and recommendations to reduce the risks linked to these weakness.

Scope

1. Zoom client meeting vulnerability affects all 40 windows desktop and laptops in use at Power plus utilities.
2. Siemens vulnerability affects 6 remote terminals spread across 3 distribution services
3. Cisco IP phone stored XSS vulnerability affects 35 Cisco SIP phones 3905 used at Power Pluse ‘s head office.

## Introduction

The Vulnerability utility report addresses the critical security concerns identified within Power Plus Utilities digital infrastructure. After a thorough comprehensive assessment, three major distinct scenario has been highlighted, each presenting unique vulnerabilities that pose significant risk to systems integrity and data confidentiality.

1. The Zoom Client Meetings prior to version 5.15.2 pose a significant threat as it imporperly neutralize special elements and allows unauthorized user to exploit network acces, leading to escalation of privilege.
2. Network configuration service in CP-8031 and CP-8050 master module device, version prior to CP185 V05,20, mishandles the conversion of 1PV4 address. This vulnerability would result in the use of uninitialized variable during subsequent validation steps, leading to potential security compromises.
3. Cisco IP Phone may be susceptible to a cross-site scripting vulnerability due to insufficient validation of user supplied input. Which may lead to an authenticated attacker with valid credentials can exploit this vulnerability.

## 

## Identification of Vulnerabilities

Power Pulse Utilities vulnerability report proves provides results of scan conducted by security department using the vulnerability scanning platform.  
   
Vulnerability #1 – Zoom Client for Meeting <5.15.2 Vulnerability (ZSB-23038)

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

Vulnerability #3 – Cisco IP stored XSS (cisco-sa-uipphone-xss-NcmUykqA)

## Analysis Using Vulnerability Databases Vulnerabilities in various sources were gathered from sources like <https://www.tenable.com/plugins/nessus> and [National Institute of Standards and Technology (nist.gov)](https://www.nist.gov/)

**Vunerability1: Zoom client for Meeting <5.15.2 Vulnerability ( ZSB-23038)**

As per CVE-2023-39213 the version prior to 5.15.2 suffer from improper neutralization of special element which allows an authenticated user to escalate privileges via network access.   
  
The NIST: NVD assigns a base score of 9.8, indicating critical severity. Whereas CNA for this vulnerability, assigns a base score of 9.6 indicating critical severity.  
  
The vulnerability affects Zoom Desktop Client for Windows and Zoom VDI Client, potentially enabling unauthorized users to exploit network access for privilege escalation. The lack of proper neutralization of special elements facilitates unauthorized elevation of privileges, potentially leading to unauthorized access, data theft, or other malicious activities.  
  
  
The CVSS V3 vector is : AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

**Vulnerability #2 Siemens (CVE-2023-42797)**  
  
As per CVE- 2023-42797 a vulnerability has been discovered in Siemens CP-8031 and CP-8050 master module, affecting all versions prior to CPCI85 V05.20. The problem resides in the network configuration of affected in 6 siemens RTU, especially in the conversion process of IPV4. This vulnerability could lead to use of uninitialized variable in subsequent validation steps. A remote attacker who is authenticated could exploit this vulnerability by uploading a special crafted network configuration data. During the device startup, code or command injection executed with root privileges could compromise the device.

The NIST: NVD assigns a base score of 7.2, indicating High severity. Whereas CNA for this vulnerability, assigns a base score of 6.6 indicating Medium severity

**Vunerability3# Cisco IP Phone Stored XSS (cisco-sa-uipphone-xss-NcmUykqA)**

A vulnerability has been identified in subset of Cisco IP phone , potentially exposing them to cross site scripting (XSS) attack. As per CVE-2023-20265 has occurred due to inadequate validation of user supplied input in web base management interface. An authenticated attacker can exploit this vulnerability by redirecting a user to malicious page containing crafted html script. This may allow attacker to gain unauthorized access to the sensitive browsed based information such as login credentials for other Web based account.

The risk assessment conducted base score from NIST which 5.4 of medium severity and Cisco to 5.5 of medium severity as well.  
  
The CVSS V3.1 vector is : AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

## Determination of Exploitability

**Vunerability1: Zoom client for Meeting <5.15.2 Vulnerability ( ZSB-23038)**No know exploits are available currently for this vulnerability as indicated in [Tenable’s plugin entry](https://www.tenable.com/plugins/nessus/184369) for this vulnerability.

**Vulnerability #2 Siemens (CVE-2023-42797)**No know exploits are available currently for this vulnerability as indicated in [Tenable’s plugin entry](https://www.tenable.com/plugins/ot/501888) for this vulnerability **Vunerability3# Cisco IP Phone Stored XSS (cisco-sa-uipphone-xss-NcmUykqA)**

No Know exploits are available for this vulnerability as indicated in [Tenable’s plugin entry](https://www.tenable.com/plugins/nessus/186612) for this vulnerability.

## 

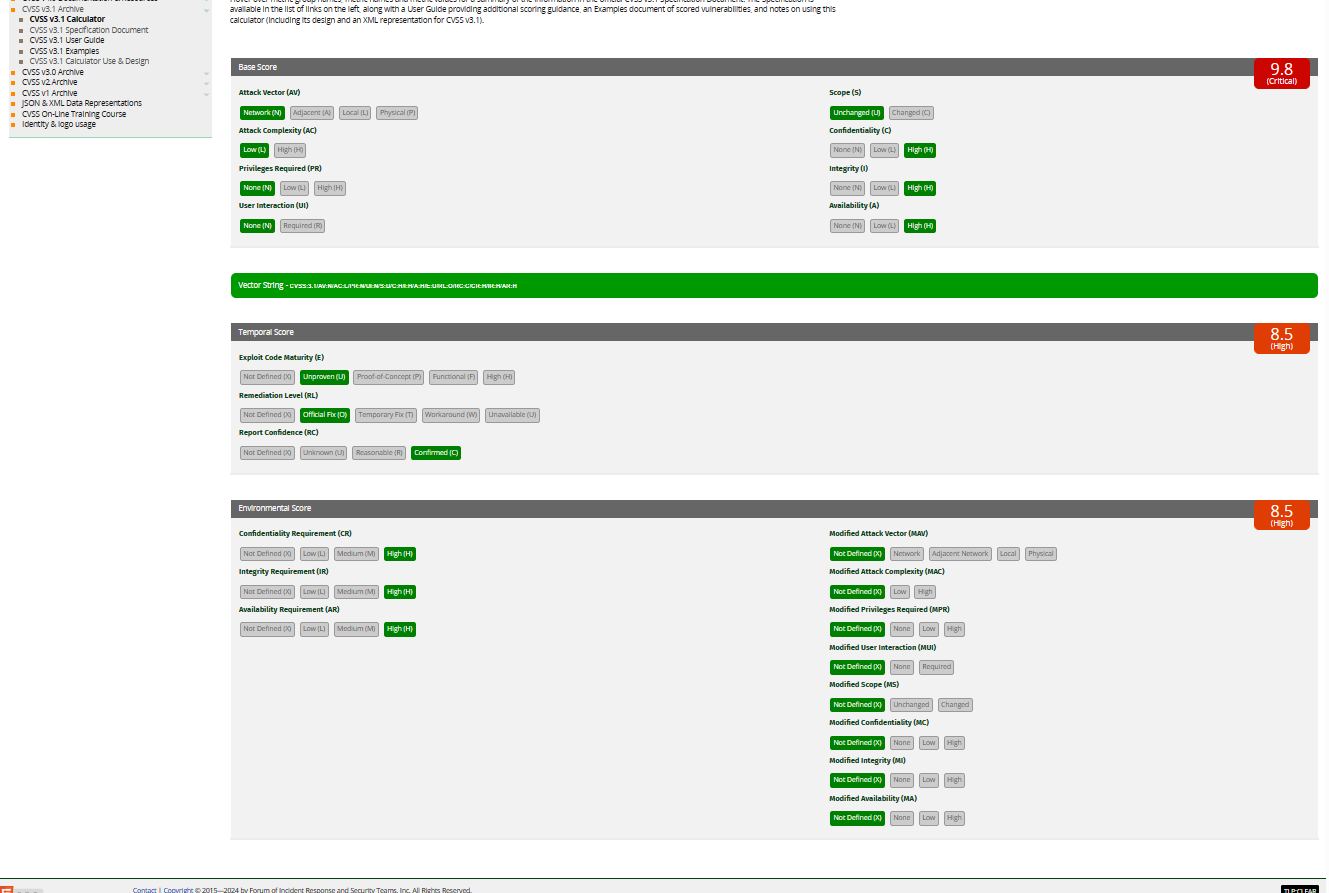
## Impact Analysis Evaluate the possible consequences for the organization if the vulnerability is leveraged. Analyze the importance of the impacted system to the operations of Power Pulse utilities. Take into account the nature of the data or operations that could be compromised.

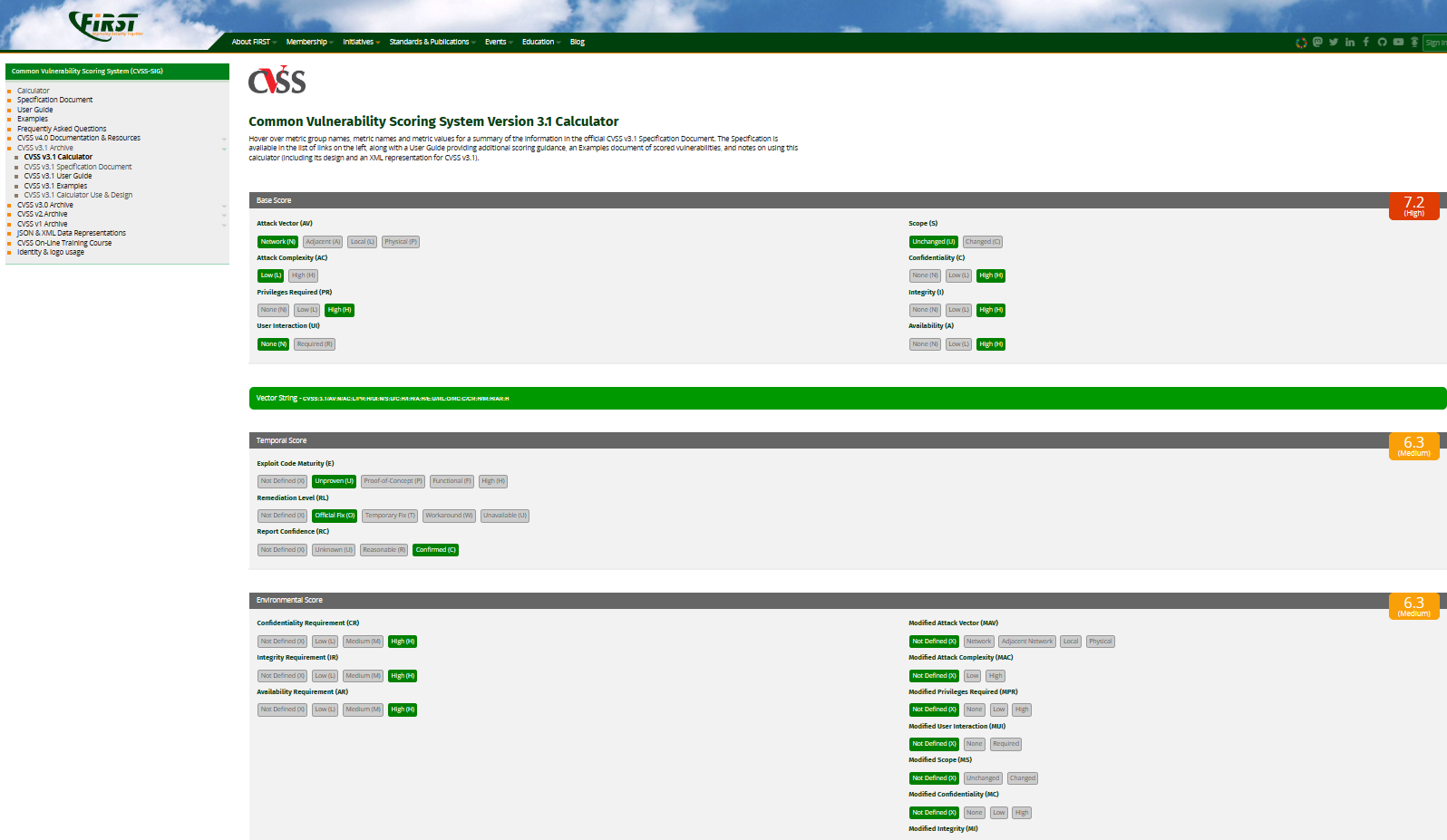
**Vunerability1: Zoom client for Meeting <5.15.2 Vulnerability ( ZSB-23038)**The vulnerability (CVE-2023-39213) found in versions prior to 5.15.2 of Zoom Desktop Client for Windows and Zoom VDI Client presents a notable risk of privilege escalation through network access. Because of inadequate handling of certain elements, an attacker without authentication could exploit this vulnerability to obtain higher privileges on the system in question. This could result in unauthorized entry, manipulation of data, or compromise of the system's integrity. While Nessus did not conduct direct testing for this vulnerability, the significance of relying solely on the application's reported version emphasizes the necessity for swift remediation efforts.

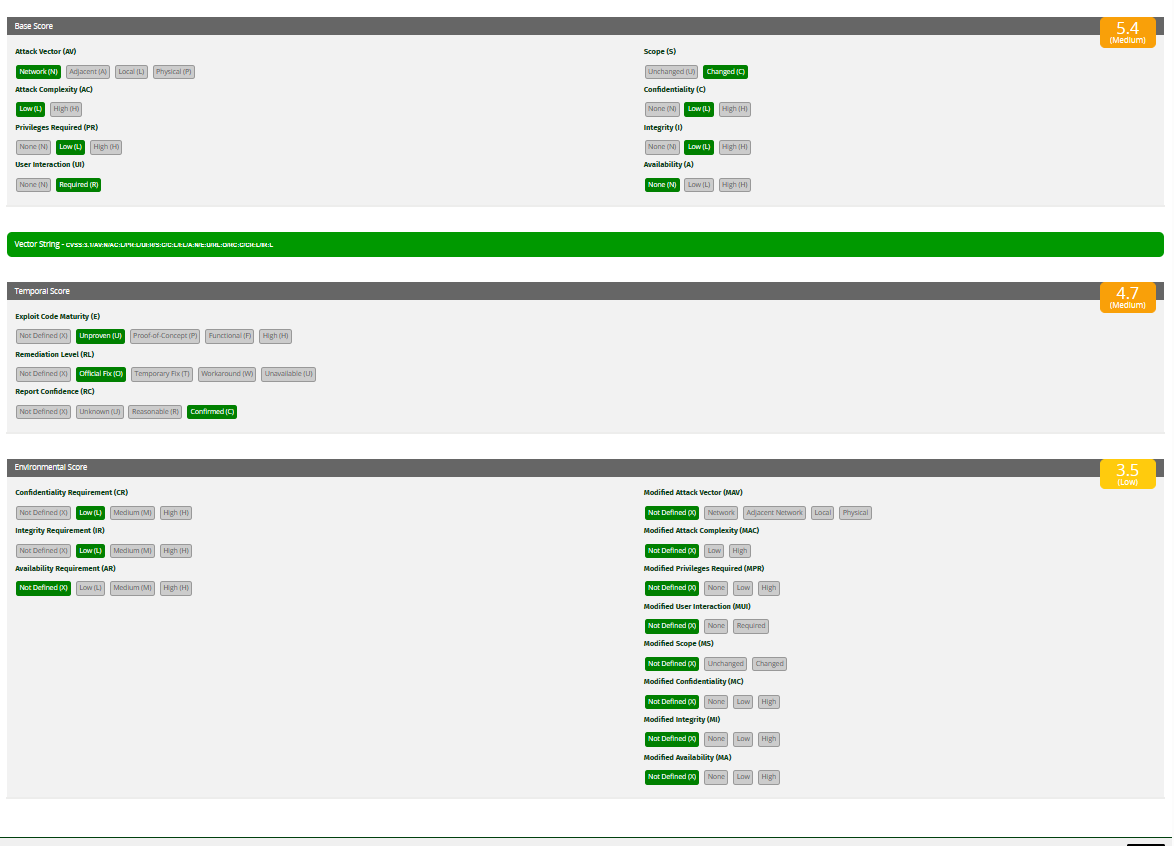
**Vulnerability #2 Siemens (CVE-2023-42797)**The vulnerability poses a high-risk scenario due to its potential for unauthorized code execution which allows authenticated remote attacker to inject command, gain root privilege escalation to gain control over the devices and gather sensitive information stored in the device leading to further exploiting the network and critical infrastructure. It may also compromise the industry regulatory compliance leadig to legal and financial repercussions. **Vunerability3# Cisco IP Phone Stored XSS (cisco-sa-uipphone-xss-NcmUykqA)**The vulnerability known as Cisco IP Phone Stored XSS presents a moderate risk, potentially leading to unauthorized entry into confidential data, alteration of device operations, impersonation of users through social engineering tactics, harm to reputation, and legal consequences due to regulatory violations. This vulnerability arises from inadequate validation of user inputs, allowing attackers to execute arbitrary script code within the interface, thereby disrupting operations, compromising user confidentiality, and accessing valuable information.

## Contextualization

The assessment of vulnerabilities should consider the specific environment they affect. For instance, a vulnerability in a development setting might pose a distinctness risk compared to the same vulnerability in a production environment. It's essential to factor in the business context, including the significance of the system within the overall business processes. Additionally, one should evaluate compensating controls that could help mitigate the risk. Adjusted scores for each vulnerability, based on Environmental Scores, have been determined using the CVSS 3.1 calculator

**Vunerability1: Zoom client for Meeting <5.15.2 Vulnerability ( ZSB-23038)**The vulnerability affects Zoom Desktop Client for Windows and Zoom VDI Client versions prior to 5.15.2. It involves improper neutralization of special elements, potentially leading to privilege escalation via network access. This means that an unauthorized user could exploit the vulnerability to gain elevated privileges on the affected system without proper authentication. Failure to adequately neutralize these vulnerabilities may enable attackers to exploit the network at the protocol level. Attackers could anticipate consistent success when targeting vulnerable components, as they possess authorization and do not need file system access to execute an attack. Additionally, the system could be compromised solely through user interaction, potentially impacting resources beyond the security perimeter. Such breaches could severely compromise the CIA triad at its highest levelThe CVSS 3.1 calculator was used to calculate an environmental score for this vulnerability. The overall severity of this vulnerability is 9.8 (Critical).  
****

**Vulnerability #2 Siemens (CVE-2023-42797)**A security vulnerability (CVE-2023-42797) has been identified in CP-8031 MASTER MODULE and CP-8050 MASTER MODULE devices running versions older than CPCI85 V05.20. This flaw in the network configuration service could potentially allow a remote attacker with authentication to inject commands with root privileges during device startup by uploading specifically crafted network configurations. Siemens advises updating affected devices to CPCI85 V05.20 or later versions and enforcing robust password policies for users authorized to modify network settings. Additionally, they recommend implementing redundant protection schemes and network access controls, and carefully validating and overseeing security updates before deployment. The risk level is evaluated as high so underlining the urgency of timely mitigation and proactive security measures to prevent potential cyber incidents affecting power grid reliability.  
  
The CVSS 3.1 calculator was used to calculate an environmental score for this vulnerability. The overall severity of this vulnerability is 7.2(Critical).  
 ****

**Vunerability3# Cisco IP Phone Stored XSS (cisco-sa-uipphone-xss-NcmUykqA)**  
The vulnerability known as Cisco IP Phone Stored XSS (CVE-2023-20265) presents a moderate risk, allowing authenticated attackers to carry out stored cross-site scripting attacks on affected device users due to insufficient validation of input in the web-based management interface. This could lead to the execution of arbitrary script code or access to sensitive browser-based data. Cisco has issued software updates to address this issue, impacting devices such as IP DECT 110/210 Base Stations, Unified IP Phone 6901, and Unified SIP Phone 3905. Unfortunately, there are no workarounds available, and affected devices must be upgraded to patched versions to ensure compatibility with hardware and software. Notably, various Cisco products, including IP Phones and conferencing systems, remain unaffected. The significance of timely mitigation is emphasized given the risk of unauthorized access and data exposure  
  
The CVSS 3.1 calculator was used to calculate an environmental score for this vulnerability. The overall severity of this vulnerability is 5.4 (Critical).  
  


## 

## Threat Environment

As per the [World Economic Forum](https://www.weforum.org/agenda/2023/10/why-the-energy-sector-and-critical-infrastructure-is-particularly-vulnerable-to-cyber-attacks/), critical infrastructure in the energy sector is undergoing rapid changes. To safeguard this infrastructure, proper measures need to be taken, considering the significant role the energy sector plays in shaping a country's economy. Energy sources like wind, solar, and nuclear power plants are increasingly reliant on digital operational technology (OT), making them susceptible to attacks. Recent trends indicate a rise in cyber threats targeting the sector, with attackers exploiting new vulnerabilities arising from digitalization. According to a 2021 survey by SANs, the energy sector is identified as the most likely target for cyber threats, with state-sponsored attackers from China, Iran, and North Korea attempting to steal crucial information from [Canadian energy](https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024) facilities.

In a recent [Forbes survey](https://www.forbes.com/sites/chuckbrooks/2023/03/05/cybersecurity-trends--statistics-for-2023-more-treachery-and-risk-ahead-as-attack-surface-and-hacker-capabilities-grow/?sh=51620b3219db), it was revealed that approximately 84% of code bases contain at least one open-source vulnerability, while phishing attacks emerged as the preferred method of attack in 2023. Both ransomware and phishing attacks are escalating, as evidenced by the fact that in 2022, 76% of organizations were targeted by ransomware attacks, resulting in 64% of them being infected. Furthermore, half of these organizations managed to retrieve their data after paying the ransom. Moreover, just over 66% of respondents reported experiencing multiple isolated infections.

Given the escalating attacks on the North American energy sector in recent years, it is imperative for Power Pulse Utilities to remain vigilant against potential threats from high-profile threat actors.

.

## Prioritization.

Power Pulse Utilities has evaluated the weaknesses and has taken into account the significance of each vulnerable asset, the characteristics of each vulnerability, and the possible consequences to the company if they are exploited. The following table provides suggested deadlines for addressing each vulnerability.

|  |  |  |
| --- | --- | --- |
| **Vulnerability#** | **Recommended Implementation Timeframe** | **Rationale** |
| 1 – Zoom Client for Meetings <5.15.2 vulnerability (ZSB-23038) | 24-48 HOURS | An unauthenticated attacker could exploit this vulnerability to gain escalated privileges on the affected systems, potentially compromising sensitive information or executing authorized actions in power pulse utility |
| 2- Siemens (CVE-2023-42797) | 14 days | Manipulate network configuration, potentially causing service disruption, unauthorized access or other security breaches on affected devices |
| 3- Cisco IP Phone Stored XSS (cisco-sa-uipphone-xss-NcmUykqA) | Within 30 days | Successful exploitation of this vulnerability could allow an attacker to compromise the CIA triad of the affected device. It could lead to unauthorized user access , data theft or other malicious activities targeting UI |

## Plan of Action

The most critical vulnerability that was assessed was Zoom Client for meeting. To fix this issue an update is required to version 5.15.2 or later to prevent this vulnerability and prevent potential privilege escalation attacks  
  
The Next vulnerability that should be assessed Siemens. To resolve this issue affected devices should be updated to CPCI85 V05.20 or later version. Additionally, customers should limit the users permitted to modify the network configuration through strong passwords.

However, the last vulnerability was Cisco IP phone that should be addressed within 30 days and to completely resolve this issue it is recommended to the user to update the software referenced in Cisco bug ID’s CSCwfr58592 for their devices to address security vulnerability. Moreover, Cisco has also confirmed that the other products not listed in the affected devices are not vulnerable to this issue

## Conclusion

In conclusion, this assessment report has identified several critical vulnerabilities within Power Pulse Utilities, including one critical, one high, and one medium priority vulnerability. If left unaddressed, these vulnerabilities could lead to unauthorized privilege escalation, service disruptions, data theft, and other significant security breaches, potentially impacting the operations and reputation of Power Pulse Utilities.

Key findings from the assessment reveal outdated versions of Zoom meeting software and Siemens Remote Terminal Units (RTUs), as well as unfixed security patches for Cisco IP phones used regularly within the organization. We recommend that Power Pulse Utilities promptly address the vulnerabilities outlined in this report, with detailed instructions provided in the Prioritization and Plan of Action section. Swiftly remedying these issues is crucial for safeguarding the organization against malicious actors and potential threats.