**Vulnerability Scan Report**

Scan Date: Jan 4th, 2024

**Vulnerability #1**

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

****

**Synopsis**

The remote host has an application installed that is affected by a vulnerability.

**Description**

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 referenced in the ZSB-23038 advisory.

- 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. (CVE-2023-39213)

**Solution**

Upgrade to Zoom Client for Meetings 5.15.2 or later.

**Scope**

This vulnerability affects all 40 windows desktops and laptops in use at PowerPulse Utilities.

**See Also**

<https://www.tenable.com/plugins/nessus/184369>

<https://www.tenable.com/cve/CVE-2023-39213>

[https://www.zoom.com/en/trust/security-bulletin/ZSB-2303](https://www.zoom.com/en/trust/security-bulletin/ZSB-23038)

<https://nvd.nist.gov/vuln/detail/CVE-2023-39213>

**Risk Information**

**CVSS v3**

**Risk Factor**: Critical

**Base Score**: 9.8

**Temporal Score**: 8.5

**Vector**:

CVSS:3.0/AV:N/AC:L.PR:N/UI:N/S:U/C:H/I:H/A:H

**Temporal Vector:** CVSS:3.0/E:U/RL:O/RC:C

**Vulnerability #2**

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

****

**Synopsis**

The remote OT asset is affected by a vulnerability.

**Description**

A vulnerability has been identified in CP-8031 MASTER MODULE (All Version , CP185 V0.5.20), CP-8050 MASTER MODULE (ALl versions < CP185 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.

**Solution**

Refer to the vendor advisory.

**Scope**

This vulnerability affects 6 Siemens Remote Terminal Units (RTUs) (Spread across 3 Distribution Stations)

**See Also**

<https://www.tenable.com/plugins/ot/501888>

<https://cert-portal.siemens.com/productcert/pdf/ssa-583634.pdf>

<https://www.tenable.com/cve/CVE-2023-42797>

<https://nvd.nist.gov/vuln/detail/CVE-2023-42797>

**Risk Information**

**CVSS v3**

**Risk Factor**: High

**Base Score**: 7.2

**Temporal Score**: 6.3

**Vector:**

CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

**Temporal Vector:** CVSS: 3.0/E:U/RL:O/RC:C

**Vulnerability #3**

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

****

**Synopsis**

The remote device may be missing a vendor-supplied security patch.

**Description**

According to its self-reported version, 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.

**Solution**

Upgrade to the relevant fixed version referenced in Cisco bug IDs CSCwfr58592, CSCwf58594

**Scope**

This vulnerability affects 35 Cisco SIP Phone 3905 used at PowerPulse’s head office.

**See Also**

[https://www.tenable.com/plugins/nessus/186612](https://www.tenable.com/plugins/186612)

<https://www.tenable.com/cve/CVE-2023-20265>

<https://nvd.nist.gov/vuln/detail/CVE-2023-20265>

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-uipphone-xss-NcmUykqA>

**Risk Information**

**CVSS v3**

**Risk Factor**: Medium

**Base Score**: 5.4

**Temporal Score**: 4.7

**Vector:**

CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:L

**Temporal Vector**: CVSS:3.0/E:U/RL:O/RC:C