Date: August 2, 2021
Subject: CVE-2021-37166
Vulnerability Name: GUI socket Denial Of Service
Vulnerability Type: Buffer overflow

Summary

A buffer overflow issue leading to denial of service was discovered in HMI-3 Control Panel in Swisslog Healthcare Nexus Panel operated by released versions of software before Nexus Software 7.2.5.7. When HMI3 starts up, it binds a local service to a TCP port on all interfaces of the device, and takes extensive time for the GUI to connect to the TCP socket, allowing the connection to be hijacked by an external attacker.

Affected Products

The following table lists the product impacted by the vulnerabilities listed above and the current state of remediation planning.

<table>
<thead>
<tr>
<th>Product</th>
<th>Fix Version</th>
<th>Target Release Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>HMI-3 Panel</td>
<td>7.2.5.7</td>
<td>August 2, 2021</td>
</tr>
</tbody>
</table>
Workaround and Mitigation

Network firewalls
Network firewalls that restrict inter-VLAN traffic on the network must allow inbound and outbound internal network connections for the ports listed in “Windows firewalls”. Do not restrict these ports to specific applications.

Layer 3 Access Control List
If there is no firewall between the SCC and the floor devices, apply an extended access control list (ACL) in the layer 3 VLAN that is dedicated to the PTS floor equipment. Both inbound and outbound access lists are required between the SCC server and floor equipment, allowing the use of the TCP and UDP ports listed.

General Security Recommendations
Swisslog Healthcare recommends upgrading to the latest software version as soon as available.

Vulnerability Classification
The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (NVD - CVSS v3 Calculator (nist.gov)). The CVSS environmental score is specific to the customer’s environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

Vulnerability CVE-2021-37166
To exploit this vulnerability, an unauthenticated attacker must be on the local network.

<table>
<thead>
<tr>
<th>CVSS v3.1 Base Score</th>
<th>9.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE Reference</td>
<td>CWE-284, CWE-400</td>
</tr>
</tbody>
</table>

Recommended Actions

1. Swisslog Healthcare recommends upgrading to the latest software version as soon as available.
2. Swisslog Healthcare recommends deploying the described mitigation methods until the updated software version is deployed.

Credits
Swisslog Healthcare would like to thank the Armis security research team in reporting this issue in a professional manner.
Support and Contact Information

Product Technical Support
- Phone 24/7 support: 800-386-9666

Report a New Security Finding
- swisslog-healthcare.com/en-us/customer-care/security-information
- Product-Security@Swisslog-Healthcare.com