



CVE-2021-37165

Published on: 08/02/2021 12:00:00 AM UTC

Last Modified on: 08/10/2021 04:46:00 PM UTC

CVE-2021-37165

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Hmi-3 Control Panel](#) from [Swisslog-healthcare](#) contain the following vulnerability:

A buffer overflow issue was discovered in HMI3 Control Panel in Swisslog Healthcare Nexus Panel operated by released versions of software before Nexus Software 7.2.5.7. When a message is sent to the HMI TCP socket, it is forwarded to the hmiProcessMsg function through the pendingQ, and may lead to remote code execution.

CVE-2021-37165 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Page could not be found - Swisslog Healthcare	www.swisslog-healthcare.com text/html Inactive Link Not Archived	MISC www.swisslog-healthcare.com/en-us/customer-care/security-information/cve-disclosures#:~:text=CVE%20Disclosures%20%20%20Vulnerability%20Name%20,%20%202021-37164%20%204%20more%20rows%20

healthcare

Medication Management: Transport, Software & Automation - Swisslog Healthcare

www.swisslog-healthcare.com
text/html

 MISC www.swisslog-healthcare.com

Page Not Found - Armis

www.armis.com
text/html

 MISC www.armis.com/PwnedPiper

www.swisslog-healthcare.com
application/pdf

 MISC www.swisslog-healthcare.com/-/media/swisslog-healthcare/documents/customer-service/armis-documents/cve-2021-37165-bulletin---overflow-in-hmiprocessmsg.pdf?rev=2e2678dab62b41ba999cd6d1e03974ca&hash=F465ACE2C7FAED826B52FE996E36ACE

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

590499 Swisslog Healthcare Translogic Pneumatic Tube Systems Multiple Vulnerabilities (ICSMA-21-215-01)

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Swisslog-healthcare	Hmi-3 Control Panel	-	All	All	All
Operating System	Swisslog-healthcare	Hmi-3 Control Panel Firmware	All	All	All	All
cpe:2.3:h:swisslog-healthcare:hmi-3_control_panel:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:swisslog-healthcare:hmi-3_control_panel_firmware:*:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-37165 : A buffer overflow issue was discovered in HMI3 Control Panel in Swisslog Healthcare Nexus Panel op... twitter.com/i/web/status/1...	2021-08-02 11:05:56
 @LinInfoSec	Nexus - CVE-2021-37165: armis.com/PwnedPiper	2021-08-02 12:41:58
 /r/sysadmin	Several zero-day PwnedPiper vulnerabilities found!	2021-08-03 08:39:36
 /r/cybersecurity	Several zero-day PwnedPiper vulnerabilities found!	2021-08-03 08:37:33
 /r/msp	Several zero-day PwnedPiper vulnerabilities found in the hospital system	2021-08-03 08:35:46

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)