SICK
Sensor Intelligence.

TLP:WHITE

SICK PSIRT
Security Advisory

Sudo vulnerability affects Endress+Hauser MCS200HW

Document ID:	SCA-2026-0007
Publication Date:	2026-04-21
CVE Identifier:	CVE-2025-32463
CVSSv3 Base Score:	9.3
CVSSv3 Vector String:	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
Version:	1.0.0

Summary

The display unit of the Endress+Hauser MCS200HW is affected by a sudo chroot vulnerability.

If exploited, this vulnerability could potentially allow an unauthenticated attacker to compromise the availability, integrity, and confidentiality of the Endress+Hauser MCS200HW.

As general security measures, SICK recommends minimizing network exposure of the devices, restricting network access, and following recommended security practices in order to operate the devices in a protected IT environment.

SICK recommends updating the display unit of the product to version 4.3.4 and ensuring that the product operates within a secure environment.

List of Products

Product	Affected by
Endress+Hauser MCS200HW with firmware <1.11.5.6R	CVE-2025-32463 Status: Known Affected Remediation: Vendor fix

Vulnerability Overview

CVE-2025-32463 Inclusion of Functionality from Untrusted Control Sphere

Vulnerability Description: Sudo before 1.9.17p1 allows local users to obtain root access because /etc/nsswitch.conf from a user-controlled directory is used with the --chroot option.

CVE-2025-32463 has been assigned to this vulnerability.
CVSSv3.1 base score: 9.3
CVSSv3.1 vector string: CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
CWE identifier: CWE-829 (Inclusion of Functionality from Untrusted Control Sphere)

Remediations

Vendor Fix for CVE-2025-32463

Details: The display unit's firmware versions below 4.3.4 are affected. To address the vulnerability, customers are strongly recommended to update the display unit of their devices to firmware version 4.3.4.
Endress+Hauser will include this firmware version in the MCS200HW products starting with version 1.11.5.6R.
Alternatively, customers can contact Endress+Hauser directly to obtain the updated display firmware, or download the original firmware - including update instructions - from the Phoenix Contact website referenced below.

Valid for:

- Endress+Hauser MCS200HW with firmware $<$1.11.5.6R

General Security Practices

General Recommendation

As general security measures, SICK recommends minimizing network exposure of the devices, restricting network access, and following recommended security practices in order to operate the devices in a protected IT environment.

Resources

Endress+Hauser:
https://www.endress.com

SICK PSIRT Security Advisories:
https://www.sick.com/psirt

ICS-CERT recommended practices on Industrial Security:
https://www.cisa.gov/resources-tools/resources/ics-recommended-practices

CVSS v3.1 Calculator:
https://www.first.org/cvss/calculator/3.1

Standalone display firmware, update procedure and further details:
https://www.phoenixcontact.com/de-de/produkte/touch-panel-wp-6121-wxps-1290802

History

Version	Release Date	Comment
1.0.0	2026-04-21	Initial version