TLP:WHITE

SICK PSIRT
Security Advisory

Vulnerability in several Endress+Hauser products

Document ID:	SCA-2026-0009
Publication Date:	2026-07-16
CVE Identifier:	CVE-2024-8751
CVSSv3 Base Score:	7.5
CVSSv3 Vector String:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Version:	1.0.0

Summary

A vulnerability was discovered in several Endress+Hauser products that can be accessed via ethernet.

If exploited, this vulnerability allows a remote unauthenticated attacker to modify the IP address of the product through the SopasET interface, potentially leading to Denial of Service. There are currently no known public exploits specifically targeting this vulnerability.

As general security measures, it is recommended to minimize network exposure of the devices, restrict network access, and follow recommended security practices in order to operate the devices in a protected IT environment.

Customers are strongly advised to apply the recommended mitigation for the affected vulnerabilities to reduce potential risk.

List of Products

Product	Affected by
Endress+Hauser FLPS all firmware versions	CVE-2024-8751 Status: Known Affected Remediation: Mitigation
Endress+Hauser GM32 all firmware versions	CVE-2024-8751 Status: Known Affected Remediation: Mitigation
Endress+Hauser GMS800 FIDOR all firmware versions	CVE-2024-8751 Status: Known Affected Remediation: Mitigation
Endress+Hauser GMS800 all firmware versions	CVE-2024-8751 Status: Known Affected Remediation: Mitigation
Endress+Hauser MARSIC200 all firmware versions	CVE-2024-8751 Status: Known Affected Remediation: Mitigation
Endress+Hauser MARSIC280 all firmware versions	CVE-2024-8751 Status: Known Affected Remediation: Mitigation
Endress+Hauser MARSIC300 all firmware versions	CVE-2024-8751 Status: Known Affected Remediation: Mitigation
Endress+Hauser MCS100FT all firmware versions	CVE-2024-8751 Status: Known Affected Remediation: Mitigation
Endress+Hauser MCS200HW all firmware versions	CVE-2024-8751 Status: Known Affected Remediation: Mitigation
Endress+Hauser MCS300P all firmware versions	CVE-2024-8751 Status: Known Affected Remediation: Mitigation
Endress+Hauser MCU ETH-Service and Modbus-TCP Module all firmware versions	CVE-2024-8751 Status: Known Affected Remediation: Mitigation

Endress+Hauser MERCEM300Z all firmware versions	CVE-2024-8751 Status: Known Affected Remediation: Mitigation
Endress+Hauser MES1B B&B Converter all firmware versions	CVE-2024-8751 Status: Known Affected Remediation: Mitigation
Endress+Hauser SAM800 all firmware versions	CVE-2024-8751 Status: Known Affected Remediation: Mitigation
Endress+Hauser SIPROCESS all firmware versions	CVE-2024-8751 Status: Known Affected Remediation: Mitigation
Endress+Hauser VICOTEC320 all firmware versions	CVE-2024-8751 Status: Known Affected Remediation: Mitigation

Vulnerability Overview

CVE-2024-8751 Missing Authentication for Critical Function

Vulnerability Description: A vulnerability allows a remote unauthenticated attacker to modify the product's IP address over the Sopas ET interface. This can lead to a Denial of Service attack.

CVE-2024-8751 has been assigned to this vulnerability.
CVSSv3.1 base score: 7.5
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CWE identifier: CWE-306 (Missing Authentication for Critical Function)

Remediations

Mitigation for CVE-2024-8751

Details: Please make sure that only trusted entities have access to the device. Furthermore, you should apply the following General Security Measures when operating the product to mitigate the associated security risk. The "ICS-CERT recommended practices on Industrial Security" could help to implement the general security practices.

Valid for:

- Endress+Hauser FLPS all firmware versions
- Endress+Hauser GM32 all firmware versions
- Endress+Hauser GMS800 FIDOR all firmware versions

- Endress+Hauser GMS800 all firmware versions
- Endress+Hauser MARSIC200 all firmware versions
- Endress+Hauser MARSIC280 all firmware versions
- Endress+Hauser MARSIC300 all firmware versions
- Endress+Hauser MCS100FT all firmware versions
- Endress+Hauser MCS200HW all firmware versions
- Endress+Hauser MCS300P all firmware versions
- Endress+Hauser MCU ETH-Service and Modbus-TCP Module all firmware versions
- Endress+Hauser MERCEM300Z all firmware versions
- Endress+Hauser MES1B B&B Converter all firmware versions
- Endress+Hauser SAM800 all firmware versions
- Endress+Hauser SIPROCESS all firmware versions
- Endress+Hauser VICOTEC320 all firmware versions

General Security Practices

General Recommendation

As general security measures, it is recommended to minimize network exposure of the devices, restrict network access, and follow 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://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

History

Version	Release Date	Comment
1.0.0	2026-07-16	Initial version