TLP:WHITE

SICK PSIRT
Security Advisory

Multiple vulnerabilities in Endress+Hauser MEAC300-FNADE4

Document ID:	SCA-2025-0008
Publication Date:	2025-07-03
CVE Identifiers:	CVE-2025-1708, CVE-2025-27449, CVE-2025-27447, CVE-2025-27448, CVE-2025-27450, CVE-2025-27451, CVE-2025-27452, CVE-2025-27453, CVE-2025-27454, CVE-2025-27455, CVE-2025-27456, CVE-2025-27457, CVE-2025-27458, CVE-2025-27459, CVE-2025-27460, CVE-2025-27461, CVE-2025-1709, CVE-2025-1710, CVE-2025-1711
Version:	1.0.0

Summary

Several vulnerabilities in the Endress+Hauser MEAC300-FNADE4 were discovered, that can be accessed via Ethernet.

If exploited, these vulnerabilities could potentially allow a remote, unauthenticated attacker to compromise the availability, integrity, and confidentiality of the MEAC300-FNADE4. SICK recommends to update the product to the newest version and ensuring the product operates within a secure environment. Currently, SICK is not aware of any exploits targeting these vulnerabilities.

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

Customers are strongly advised to update to the newest version.

List of Products

Product	Affected by
Endress+Hauser MEAC300-FNADE4 all firmware versions	CVE-2025-27456 Status: Known Affected Remediation: Mitigation
	CVE-2025-27457 Status: Known Affected Remediation: Mitigation
	CVE-2025-27458 Status: Known Affected Remediation: Mitigation
	CVE-2025-27459 Status: Known Affected Remediation: Mitigation
	CVE-2025-27460 Status: Known Affected Remediation: Mitigation
	CVE-2025-27461 Status: Known Affected Remediation: Mitigation
Endress+Hauser MEAC300-FNADE4 with Firmware <=0.16.0	CVE-2025-1708 Status: Known Affected Remediation: Vendor fix
	CVE-2025-27449 Status: Known Affected Remediation: Vendor fix
	CVE-2025-27447 Status: Known Affected Remediation: Vendor fix
	CVE-2025-27448 Status: Known Affected Remediation: Vendor fix
	CVE-2025-27450 Status: Known Affected Remediation: Vendor fix

	CVE-2025-27451 Status: Known Affected Remediation: Vendor fix
	CVE-2025-27452 Status: Known Affected Remediation: Vendor fix
	CVE-2025-27453 Status: Known Affected Remediation: Vendor fix
	CVE-2025-27454 Status: Known Affected Remediation: Vendor fix
	CVE-2025-27455 Status: Known Affected Remediation: Vendor fix
	CVE-2025-1709 Status: Known Affected Remediation: Vendor fix
	CVE-2025-1710 Status: Known Affected Remediation: Vendor fix
	CVE-2025-1711 Status: Known Affected Remediation: Vendor fix

Vulnerability Overview

CVE-2025-1708 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability Description: The application is vulnerable to SQL injection attacks. An attacker is able to dump the PostgreSQL database and read its content.

CVE-2025-1708 has been assigned to this vulnerability.
CVSSv3.1 base score: 8.6
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N
CWE identifier: CWE-89 (Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'))

CVE-2025-27449 Improper Restriction of Excessive Authentication Attempts

Vulnerability Description: The MEAC300-FNADE4 does not implement sufficient measures to prevent multiple failed authentication attempts within a short time frame, making it susceptible to brute-force attacks.

CVE-2025-27449 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:H/I:N/A:N
CWE identifier: CWE-307 (Improper Restriction of Excessive Authentication Attempts)

CVE-2025-27447 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Vulnerability Description: The web application is susceptible to cross-site-scripting attacks. An attacker can create a prepared URL, which injects JavaScript code into the website. The code is executed in the victim's browser when an authenticated administrator clicks the link.

CVE-2025-27447 has been assigned to this vulnerability.
CVSSv3.1 base score: 7.4
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N
CWE identifier: CWE-79 (Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'))

CVE-2025-27448 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Vulnerability Description: The web application is susceptible to cross-site-scripting attacks. An attacker who can create new dashboards can inject JavaScript code into the dashboard name which will be executed when the website is loaded.

CVE-2025-27448 has been assigned to this vulnerability.
CVSSv3.1 base score: 6.8
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N
CWE identifier: CWE-79 (Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'))

CVE-2025-27450 Sensitive Cookie in HTTPS Session Without 'Secure' Attribute

Vulnerability Description: The Secure attribute is missing on multiple cookies provided by the MEAC300-FNADE4. An attacker can trick a user to establish an unencrypted HTTP connection to the server and intercept the request containing the PHPSESSID cookie.

CVE-2025-27450 has been assigned to this vulnerability.
CVSSv3.1 base score: 6.5
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N
CWE identifier: CWE-614 (Sensitive Cookie in HTTPS Session Without 'Secure' Attribute)

CVE-2025-27451 Observable Response Discrepancy

Vulnerability Description: For failed login attempts, the application returns different error messages depending on whether the login failed due to an incorrect password or a non-existing username. This allows an attacker to guess usernames until they find an existing one.

CVE-2025-27451 has been assigned to this vulnerability.
CVSSv3.1 base score: 5.3
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
CWE identifier: CWE-204 (Observable Response Discrepancy)

CVE-2025-27452 Exposure of Information Through Directory Listing

Vulnerability Description: The configuration of the Apache httpd webserver which serves the MEAC300-FNADE4 web application, is partly insecure. There are modules activated that are not required for the operation of the FNADE4 web application. The functionality of the some modules pose a risk to the webserver which enable dircetory listing.

CVE-2025-27452 has been assigned to this vulnerability.
CVSSv3.1 base score: 5.3
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
CWE identifier: CWE-548 (Exposure of Information Through Directory Listing)

CVE-2025-27453 Sensitive Cookie Without 'HttpOnly' Flag

Vulnerability Description: The HttpOnly flag is set to false on the PHPSESSION cookie. Therefore, the cookie can be accessed by other sources such as JavaScript.

CVE-2025-27453 has been assigned to this vulnerability.
CVSSv3.1 base score: 5.3
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N
CWE identifier: CWE-1004 (Sensitive Cookie Without 'HttpOnly' Flag)

CVE-2025-27454 Cross-Site Request Forgery (CSRF)

Vulnerability Description: The application is vulnerable to cross-site request forgery. An attacker can trick a valid, logged in user into submitting a web request that they did not intend. The request uses the victim's browser's saved authorization to execute the request.

CVE-2025-27454 has been assigned to this vulnerability.
CVSSv3.1 base score: 4.3
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N
CWE identifier: CWE-352 (Cross-Site Request Forgery (CSRF))

CVE-2025-27455 Improper Restriction of Rendered UI Layers or Frames

Vulnerability Description : The web application is vulnerable to clickjacking attacks. The site can be embedded into another frame, allowing an attacker to trick a user into clicking on something different from what the user perceives, thus potentially revealing confidential information or allowing others to take control of their computer while clicking on seemingly innocuous objects.

CVE-2025-27455 has been assigned to this vulnerability.
CVSSv3.1 base score: 4.3
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N
CWE identifier: CWE-1021 (Improper Restriction of Rendered UI Layers or Frames)

CVE-2025-27456 Improper Restriction of Excessive Authentication Attempts

Vulnerability Description : The SMB server's login mechanism does not implement sufficient measures to prevent multiple failed authentication attempts within a short time frame, making it susceptible to brute-force attacks.

CVE-2025-27456 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:H/I:N/A:N
CWE identifier: CWE-307 (Improper Restriction of Excessive Authentication Attempts)

CVE-2025-27457 Cleartext Transmission of Sensitive Information

Vulnerability Description : All communication between the VNC server and client(s) is unencrypted. This allows an attacker to intercept the traffic and obtain sensitive data.

CVE-2025-27457 has been assigned to this vulnerability.
CVSSv3.1 base score: 6.5
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N
CWE identifier: CWE-319 (Cleartext Transmission of Sensitive Information)

CVE-2025-27458 Use of a Broken or Risky Cryptographic Algorithm

Vulnerability Description : The VNC authentication mechanism bases on a challenge-response system where both server and client use the same password for encryption. The challenge is sent from the server to the client, is encrypted by the client and sent back. The server does the same encryption locally and if the responses match it is prooven that the client knows the correct password. Since all VNC communication is unencrypted, an attacker can obtain the challenge and response and try to derive the password from this information.

CVE-2025-27458 has been assigned to this vulnerability.
CVSSv3.1 base score: 6.5
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N
CWE identifier: CWE-327 (Use of a Broken or Risky Cryptographic Algorithm)

CVE-2025-27459 Storing Passwords in a Recoverable Format

Vulnerability Description : The VNC application stores its passwords encrypted within the registry but uses DES for encryption. As DES is broken, the original passwords can be recovered.

CVE-2025-27459 has been assigned to this vulnerability.
CVSSv3.1 base score: 4.4
CVSSv3.1 vector string: CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N
CWE identifier: CWE-257 (Storing Passwords in a Recoverable Format)

CVE-2025-27460 Cleartext Storage of Sensitive Information

Vulnerability Description : The hard drives of the device are not encrypted using a full volume encryption feature such as BitLocker. This allows an attacker with physical access to the device to use an alternative operating system to interact with the hard drives, completely circumventing the Windows login. The attacker can read from and write to all files on the hard drives.

CVE-2025-27460 has been assigned to this vulnerability.
CVSSv3.1 base score: 7.6
CVSSv3.1 vector string: CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
CWE identifier: CWE-312 (Cleartext Storage of Sensitive Information)

CVE-2025-27461 Missing Authorization

Vulnerability Description : During startup, the device automatically logs in the EPC2 Windows user without requesting a password.

CVE-2025-27461 has been assigned to this vulnerability.
CVSSv3.1 base score: 7.6
CVSSv3.1 vector string: CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
CWE identifier: CWE-862 (Missing Authorization)

CVE-2025-1709 Plaintext Storage of a Password

Vulnerability Description : Several credentials for the local PostgreSQL database are stored in plain text (partially base64 encoded).

CVE-2025-1709 has been assigned to this vulnerability.
CVSSv3.1 base score: 6.5
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
CWE identifier: CWE-256 (Plaintext Storage of a Password)

CVE-2025-1710 Improper Restriction of Excessive Authentication Attempts

Vulnerability Description : The maxView Storage Manager does not implement sufficient measures to prevent multiple failed authentication attempts within a short time frame, making it susceptible to brute-force attacks.

CVE-2025-1710 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:H/I:N/A:N
CWE identifier: CWE-307 (Improper Restriction of Excessive Authentication Attempts)

CVE-2025-1711 Use of Default Credentials

Vulnerability Description : Multiple services of the DUT as well as different scopes of the same service reuse the same credentials.

CVE-2025-1711 has been assigned to this vulnerability.
CVSSv3.1 base score: 4.3
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N
CWE identifier: CWE-1392 (Use of Default Credentials)

Remediations

Vendor Fix for CVE-2025-1708

Details: Customers are strongly advised to update to the newest version.

Valid for:

- Endress+Hauser MEAC300-FNADE4 with Firmware <=0.16.0

Vendor Fix for CVE-2025-27449

Details: Customers are strongly advised to update to the newest version.

Valid for:

- Endress+Hauser MEAC300-FNADE4 with Firmware <=0.16.0

Vendor Fix for CVE-2025-27447

Details: Customers are strongly advised to update to the newest version.

Valid for:

- Endress+Hauser MEAC300-FNADE4 with Firmware <=0.16.0

Vendor Fix for CVE-2025-27448

Details: Customers are strongly advised to update to the newest version.

Valid for:

- Endress+Hauser MEAC300-FNADE4 with Firmware <=0.16.0

Vendor Fix for CVE-2025-27450

Details: Customers are strongly advised to update to the newest version.

Valid for:

- Endress+Hauser MEAC300-FNADE4 with Firmware <=0.16.0

Vendor Fix for CVE-2025-27451

Details: Customers are strongly advised to update to the newest version.

Valid for:

- Endress+Hauser MEAC300-FNADE4 with Firmware <=0.16.0

Vendor Fix for CVE-2025-27452

Details: Customers are strongly advised to update to the newest version.

Valid for:

- Endress+Hauser MEAC300-FNADE4 with Firmware <=0.16.0

Vendor Fix for CVE-2025-27453

Details: Customers are strongly advised to update to the newest version.

Valid for:

- Endress+Hauser MEAC300-FNADE4 with Firmware <=0.16.0

Vendor Fix for CVE-2025-27454

Details: Customers are strongly advised to update to the newest version.

Valid for:

- Endress+Hauser MEAC300-FNADE4 with Firmware <=0.16.0

Vendor Fix for CVE-2025-27455

Details: Customers are strongly advised to update to the newest version.

Valid for:

- Endress+Hauser MEAC300-FNADE4 with Firmware <=0.16.0

Mitigation for CVE-2025-27456

Details: Please make sure that you apply general security practices when operating the MEAC300-FNADE4. The following General Security Practices could mitigate the associated security risk.

Valid for:

- Endress+Hauser MEAC300-FNADE4 all firmware versions

Mitigation for CVE-2025-27457

Details: Please make sure that you apply general security practices when operating the MEAC300-FNADE4. The following General Security Practices could mitigate the associated security risk.

Valid for:

- Endress+Hauser MEAC300-FNADE4 all firmware versions

Mitigation for CVE-2025-27458

Details: Please make sure that you apply general security practices when operating the MEAC300-FNADE4. The following General Security Practices could mitigate the associated security risk.

Valid for:

- Endress+Hauser MEAC300-FNADE4 all firmware versions

Mitigation for CVE-2025-27459

Details: Please make sure that you apply general security practices when operating the MEAC300-FNADE4. The following General Security Practices could mitigate the associated security risk.

Valid for:

- Endress+Hauser MEAC300-FNADE4 all firmware versions

Mitigation for CVE-2025-27460

Details: Please make sure that you apply general security practices when operating the MEAC300-FNADE4. The following General Security Practices could mitigate the associated security risk.

Valid for:

- Endress+Hauser MEAC300-FNADE4 all firmware versions

Mitigation for CVE-2025-27461

Details: Please make sure that you apply general security practices when operating the MEAC300-FNADE4. The following General Security Practices could mitigate the associated security risk.

Valid for:

- Endress+Hauser MEAC300-FNADE4 all firmware versions

Vendor Fix for CVE-2025-1709

Details: Customers are strongly advised to update to the newest version.

Valid for:

- Endress+Hauser MEAC300-FNADE4 with Firmware <=0.16.0

Vendor Fix for CVE-2025-1710

Details: Customers are strongly advised to update to the newest version.

Valid for:

- Endress+Hauser MEAC300-FNADE4 with Firmware <=0.16.0

Vendor Fix for CVE-2025-1711

Details: Customers are strongly advised to update to the newest version.

Valid for:

- Endress+Hauser MEAC300-FNADE4 with Firmware <=0.16.0

General Security Practices

General Recommendation

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

Resources

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

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	2025-07-03	Initial version