Endress+Hauser
People for Process Automation

Endress+Hauser: Multiple vulnerabilities in MEAC300-FNADE4

Advisory ID
VDE-2025-036

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

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

Impact
If exploited, these vulnerabilities could potentially allow a remote, unauthenticated attacker to compromise the availability, integrity, and confidentiality of the MEAC300-FNADE4.

Vulnerability Description

CVE Number	CVSS v3.1 base score:	Description
CVE-2025-1708	**8.6 high** (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'). The application is vulnerable to SQL injection attacks. An attacker is able to dump the PostgreSQL database and read its content.
CVE-2025-27449	**7.5 high** (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)	CWE-307: Improper Restriction of Excessive Authentication Attempts. 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-2025-27447	**7.4 high** (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'). 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-2025-27448	**6.8 medium** (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N)	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'). 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-2025-27450	**6.5 medium** (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N)	CWE-614: Sensitive Cookie in HTTPS Session Without 'Secure' Attribute. 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-2025-27451	**5.3 medium** (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)	CWE-204: Observable Response Discrepancy. 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-2025-27452	**5.3 medium** (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)	CWE-548: Exposure of Information Through Directory Listing. 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-2025-27453	**5.3 medium** (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N)	CWE-1004: Sensitive Cookie Without 'HttpOnly' Flag. The HttpOnly flag is set to false on the PHPSESSION cookie. Therefore, the cookie can be accessed by other sources such as JavaScript.
CVE-2025-27454	**4.3 medium** (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N)	CWE-352: Cross-Site Request Forgery (CSRF). 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-2025-27455	**4.3 medium** (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N)	CWE-1021: Improper Restriction of Rendered UI Layers or Frames. 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-2025-1709	**6.5 medium** (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N)	CWE-256: Plaintext Storage of a Password. Several credentials for the local PostgreSQL database are stored in plain text (partially base64 encoded).

CVE-2025-1710	**7.5 high** (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)	CWE-307: Improper Restriction of Excessive Authentication Attempts. 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-2025-1711	**4.3 medium** (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N)	CWE-1392: Use of Default Credentials. Multiple services of the DUT as well as different scopes of the same service reuse the same credentials.

Affected Products

Product Name	Affected Firmware Versions
MEAC300-FNADE4	≤ FW 0.16.0

Remediation

Endress+Hauser provides updated firmware version which fixes the vulnerability. Endress+Hauser strongly recommends customers to update to the new fixed version. For support, please contact your local service center.

Vulnerability Description

CVE Number	CVSS v3.1 base score:	Description
CVE-2025-27456	**7.5 high** (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)	CWE-307: Improper Restriction of Excessive Authentication Attempts. 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-2025-27457	**6.5 medium** (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N)	CWE-319: Cleartext Transmission of Sensitive Information. All communication between the VNC server and client(s) is unencrypted. This allows an attacker to intercept the traffic and obtain sensitive data.
CVE-2025-27458	**6.5 medium** (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N)	CWE-327: Use of a Broken or Risky Cryptographic Algorithm. 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 proven 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-2025-27459	**4.4 medium** (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N)	CWE-257: Storing Passwords in a Recoverable Format. 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-2025-27460	**7.6 high** (CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)	CWE-312: Cleartext Storage of Sensitive Information. 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-2025-27461	**7.6 high** (CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)	CWE-862: Missing Authorization. During startup, the device automatically logs in the EPC2 Windows user without requesting a password.

Affected Products

Product Name	Affected Firmware Versions
MEAC300-FNADE4	all

Temporary Fix/ Mitigation

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

General Security Practices

As general security measures, Endress+Hauser 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.