VEGA: Unsecured Configuration Interface Allows Unauthorized Access Leading to Privilege Escalation

VDE-2026-016

Last update	04/22/2026 11:00
Published at	04/22/2026 11:00
Vendor(s)	VEGA Grieshaber KG
External ID	VDE-2026-016
CSAF Document	Download ↗

Summary

Vulnerable components expose sensitive information to unauthorized actors through an unsecured configuration interface. Vulnerable firmware releases contain an unsecured configuration interface that allows retrieval of sensitive information such as hashed credentials.

It was found that users with no or low rights can access information from devices that should not be available to them.

An attacker can use this information to impersonate authorized users.

Impact

An unauthenticated attacker can obtain sensitive information, potentially enabling authenticated device modification.

Affected Product(s)

Model no.	Product name	Affected versions
PS6X.???????????? Y????????	VEGAPULS 6X Two-wire PROFINET, Modbus TCP, OPC UA (Ethernet-APL)	Firmware 1.0.0, Firmware 1.1.0

Vulnerabilities

Expand / Collapse all

CVE-2026-3323 7.5

Mitigation

Implement access controls for physical interfaces to prevent unauthorized access.

Remediation

Update to the fixed firmware versions listed in this advisory. Rotate any credentials used on affected devices as they may have been compromised. Contact VEGA Support if emergency code rotation is necessary based on your risk assessment.

Acknowledgments

VEGA Grieshaber KG thanks the following parties for their efforts:

- CERT@VDE for coordination (see https://certvde.com ↗)
- Product Security Unit at VEGA Grieshaber KG for reporting (see https://www.vega.com ↗)

Revision History

Version	Date	Summary
1.0.0	04/22/2026 11:00	Initial version