VDE-2026-121: Phoenix Contact: GSDX SignatureValue verification, signed plug-in validation bypass and path traversal vulnerabilities in PLCnext Engineer programming software

Publisher: Phoenix Contact GmbH & Co. KG	Document category: csaf_security_advisory
Initial release date: Wed Nov 04 11:00:00 CET 2026	Engine: 2.6.16
Current release date: Wed Nov 04 11:00:00 CET 2026	Build Date: Tue Oct 27 11:07:24 CET 2026
Current version: 1.0.0	Status: FINAL
CVSSv3.1 Base Score: 8.4	Severity: High
Original language:	Language: en-GB
Also referred to: VDE-2026-121, PCSA-2026-00016	

Summary

GSDX SignatureValue verification, signed plug-in validation bypass and path traversal vulnerabilities have been identified in PLCnext Engineer prior to version 2026.6. The effects of these vulnerabilities may result in a complete loss of confidentiality, integrity and availability.

Impact

GSDX (Signature Verification Bypass):

This vulnerability can lead to tampered PROFINET device descriptions (GSDML) being imported and displayed as cryptographically valid because the signature value is never verified against the signer's public key. As a result, manipulated module definitions, parameter limits, or device configurations can propagate into engineering projects and be deployed to PROFINET IO controllers and field devices without any indication of tampering.

PFI (Plugin Deployment Signature Bypass):

This vulnerability can lead to arbitrary code execution in the context of the PLCnext Engineer user because unsigned archive entries outside the signed prefix are deployed and overwrite verified plugin assemblies while the package still passes signature verification.

PFI (Path Traversal in Plugin Deployment):

The plugin deployment routine does not validate path components when extracting archive entries. A crafted plugin package containing relative path segments can write files outside the plugin repository to arbitrary locations accessible with the current user's permissions.

© Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8, D-32825 Blomberg, Germany

Mitigation

Phoenix Contact recommends to install plugins only from trusted sources and verified engineering libraries. To mitigate the GSDX vulnerability we recommend to use external tools to verify the signature.

Remediation

Phoenix Contact strongly recommends to upgrade to PLCnext Engineer 2026.6 which fixes these vulnerabilities.

Acknowledgments

Phoenix Contact GmbH & Co. KG thanks the following parties for their efforts:

- CERTVDE for coordination. (see: https://certvde.com/en/)
- Ievgen Bondarenko for reporting.

Phoenix Contact GmbH & Co. KG

Namespace: https://phoenixcontact.com/psirt

psirt@phoenixcontact.com

References

- pcsa-2026-00016 (EXTERNAL): https://phoenixcontact.com/psirt
- Phoenix Contact advisory overview at CERT@VDE (EXTERNAL): https://certvde.com/de/advisories/vendor/phoenixcontact/
- VDE-2026-121: Phoenix Contact: GSDX SignatureValue verification, signed plug-in validation bypass and path traversal vulnerabilities in PLCnext Engineer programming software - HTML (SELF): https://certvde.com/en/advisories/VDE-2026-121
- VDE-2026-121: Phoenix Contact: GSDX SignatureValue verification, signed plug-in validation bypass and path traversal vulnerabilities in PLCnext Engineer programming software - CSAF (SELF): https://phoenixcontact.csaf-tp.certvde.com/.well-known/csaf/white/2026/vde-2026-121.json
- Phoenix Contact application note (EXTERNAL): https://dam-mdc.phoenixcontact.com/asset/156443151564/0a870ae433c19148b80bd760f3a1c1f2/107913_en_03.pdf

Revision history

Version	Date of the revision	Summary of the revision
1.0.0	Wed Oct 14 09:41:04 CEST 2026	Initial revision.

© Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8, D-32825 Blomberg, Germany

Sharing rules

TLP:WHITE
For the TLP version see https://www.first.org/tlp/

© Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8, D-32825 Blomberg, Germany

Vulnerability Details

Missing GSDX SignatureValue verification (CVE-2026-110021)

CVE description

PLCnext Engineer checks GSDX manifest reference digests but does not cryptographically verify the XML SignatureValue over canonicalized SignedInfo. An unauthenticated local attacker can modify signed GSDML content, update its manifest digest, retain the public certificate data, and leave an invalid nonempty SignatureValue. PLCnext Engineer prior to 2026.6 reports the package as Valid and selects the modified device description for import under the default policy.

CWE:	CWE-347: Improper Verification of Cryptographic Signature

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
PLCnext Engineer <2026.6 Order number: 1046008	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N	6.2

Fixed

Product
PLCnext Engineer 2026.6 Order number: 1046008 (Download)

Acknowledgments

- Ievgen Bondarenko for reporting.

References

- CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N - 6.9 / Medium (EXTERNAL): https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:N/VI:H/VA:N/SC:N/SI:N/S

Signed plug-in validation bypass (CVE-2026-110022)

CVE description

The PFI plugin framework deploys executable assemblies (DLLs) from a signed plugin package into the local plugin repository and loads them via reflection, but the deployment routine processes archive entries that were never covered by the signature verification. An unauthenticated local attacker can replace an

© Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8, D-32825 Blomberg, Germany

unsigned DLL outside the signed prefix in the archive passes verification and overwrites the legitimate signed assembly at the same destination path. The plugin loader then instantiates the attacker-supplied code without any additional integrity check resulting in a full compromise of the affected systems.

CWE:	CWE-494: Download of Code Without Integrity Check

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
PLCnext Engineer <2026.6 Order number: 1046008	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	8.4

Fixed

Product
PLCnext Engineer 2026.6 Order number: 1046008 (Download)

Acknowledgments

- Ievgen Bondarenko for reporting.

References

- CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N - 8.6 / High (EXTERNAL): https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/S

Path traversal in plug-in deployment (CVE-2026-110935)

CVE description

The PFI plugin framework deployment routine does not validate path components when extracting archive entries to the local plugin repository. Archive entries containing relative path segments such as '..' are not rejected, allowing an unauthenticated local attacker to write files outside the plugin repository to arbitrary locations accessible with the current user's permissions which could result in full system compromise.

CWE:	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Product status

© Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8, D-32825 Blomberg, Germany

Known affected

Product	CVSS-Vector	CVSS Base Score
PLCnext Engineer <2026.6 Order number: 1046008	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	8.4

Fixed

Product
PLCnext Engineer 2026.6 Order number: 1046008 (Download)

Acknowledgments

- Ievgen Bondarenko for reporting.

References

- CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N - 8.6 / High (EXTERNAL): https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/S

© Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8, D-32825 Blomberg, Germany