TLP:WHITE

VDE-2024-067: Phoenix Contact: Multiple Vulnerabilities in PLCnext Engineer

Publisher: Phoenix Contact GmbH & Co. KG	Document category: csaf_security_advisory
Initial release date: Tue Oct 08 12:00:00 CEST 2024	Engine: 2.5.12
Current release date: Tue Oct 08 12:00:00 CEST 2024	Build Date: Wed Oct 02 11:55:24 CEST 2024
Current version: 1	Status: FINAL
CVSSv3.1 Base Score: 7.5	Severity: High
Original language: en	Language: en-GB
Also referred to: VDE-2024-067, PCSA-2024/00013	

Summary

Vulnerabilities in .NET and Visual Studio functions System.Text.Json, System.Formats.Asn1, OPCFoundation.NetStandard.Opc.Ua.Core allow an remote attacker to execute a Denial-of-Servce attack.

General Recommendation

For general information and recommendations on security measures to protect network-enabled\ndevices, refer to the application note: Application Note Security.

Impact

Availability of an application programming workstation might be compromised by attacks using these vulnerabilities.

Mitigation

To mitigate the vulnerabilities and to ensure the availability of the PLCnext Engineer please ensure that only data from trusted sources are used.

Remediation

Phoenix Contact recommends affected users to update to the current PLCnext Engineer 2024.0.4 LTS or 2024.6 which fixes the vulnerabilities.

Product Description

Engineering software platform for Phoenix Contact automation controllers. PLCnext Engineer is IEC 61131-3-compliant.

Summary

Vulnerabilities in .NET and Visual Studio functions System.Text.Json, System.Formats.Asn1, OPCFoundation.NetStandard.Opc.Ua.Core allow an remote attacker to execute a Denial-of-Servce attack.

Product groups

Affected Products IDs

- PLCnext Engineer < 2024.0.4 LTS
- PLCnext Engineer < 2024.6

Fixed Product IDs

- PLCnext Engineer 2024.0.4 LTS
- PLCnext Engineer 2024.6

Vulnerabilities

CVE-2024-30105 (CVE-2024-30105)

Description

.NET Core and Visual Studio Denial of Service Vulnerability.
Details: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30105

CWE: CWE-400: Uncontrolled Resource Consumption

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
PLCnext Engineer < 2024.0.4 LTS Order number: 1046008	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
PLCnext Engineer < 2024.6 Order number: 1046008	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5

Fixed

Product
PLCnext Engineer 2024.0.4 LTS Order number: 1046008 (Download)
PLCnext Engineer 2024.6 Order number: 1046008 (Download)

Remediations

Vendor fix

Phoenix Contact recommends affected users to update to the current PLCnext Engineer 2024.0.4 LTS or 2024.6 which fixes the vulnerabilities.

For groups:

- Affected Products IDs

CVE-2024-33862 (CVE-2024-33862)

Description

A buffer-management vulnerability in OPC Foundation OPCFoundation.NetStandard.Opc.Ua.Core before 1.05.374.54 could allow remote attackers to exhaust memory resources. It is triggered when the system receives an excessive number of messages from a remote source. This could potentially lead to a denial of service (DoS) condition, disrupting the normal operation of the system.

Details: https://files.opcfoundation.org/SecurityBulletins/OPC%20Foundation%20Security%20Bulletin%20CVE-2024-33862.pdf

CWE: CWE-770: Allocation of Resources Without Limits or Throttling

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
PLCnext Engineer < 2024.0.4 LTS Order number: 1046008	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
PLCnext Engineer < 2024.6 Order number: 1046008	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5

Fixed

Product
PLCnext Engineer 2024.0.4 LTS Order number: 1046008 (Download)
PLCnext Engineer 2024.6 Order number: 1046008 (Download)

Remediations

Vendor fix

Phoenix Contact recommends affected users to update to the current PLCnext Engineer 2024.0.4 LTS or 2024.6 which fixes the vulnerabilities.

For groups:

- Affected Products IDs

CVE-2024-38095 (CVE-2024-38095)

Description

.NET and Visual Studio Denial of Service Vulnerability.
Details: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38095

CWE: CWE-20: Improper Input Validation

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
PLCnext Engineer < 2024.0.4 LTS Order number: 1046008	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
PLCnext Engineer < 2024.6 Order number: 1046008	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5

Fixed

Product
PLCnext Engineer 2024.0.4 LTS Order number: 1046008 (Download)
PLCnext Engineer 2024.6 Order number: 1046008 (Download)

Remediations

Vendor fix

Phoenix Contact recommends affected users to update to the current PLCnext Engineer 2024.0.4 LTS or 2024.6 which fixes the vulnerabilities.

For groups:

- Affected Products IDs

Acknowledgments

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

- CERT@VDE for the coordination and support with this publication. (see: https://certvde.com)

Phoenix Contact GmbH & Co. KG

Namespace: https://phoenixcontact.com/psirt

https://phoenixcontact.com/psirt

References

- PCSA-2024/00013 (EXTERNAL): https://phoenixcontact.com/psirt
- Phoenix Contact advisory overview at CERT@VDE (EXTERNAL): https://cert.vde.com/de/advisories/vendor/phoenixcontact/
- Phoenix Contact application note (EXTERNAL): https://dam-mdc.phoenixcontact.com/asset/156443151564/0a870ae433c19148b80bd760f3a1c1f2/107913_en_03.pdf
- VDE-2024-067: Phoenix Contact: Multiple Vulnerabilities in PLCnext Engineer (SELF): https://cert.vde.com/en/advisories/VDE-2024-067/

Revision history

Version	Date of the revision	Summary of the revision
1	Tue Oct 08 12:00:00 CEST 2024	A new PLCnext Engineer releases fixes known vulnerabilities in open-source libraries utilized by PLCnext Engineer.

Sharing rules

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