OPC Foundation Security Bulletin

Security Update for the OPC UA .NET Standard Stack

Published: February 9th, 2025
Version: 1.0

Executive Summary

This security update resolves a vulnerability in the OPC UA .NET Standard Stack that allows an unauthorized attacker to bypass application authentication when using HTTPS endpoints.

This security update has a base score of 6.5 (Medium) using the CVSS v3.1 guidelines.

The CVSS vector string is:
CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N

Affected Software

The following software has been updated to address the issue:

Download		Replacement
OPCFoundation/UA-.NETStandard		
This version or any version after it.		1.5.374.158 GitHub Commit: https://github.com/OPCFoundation/UA-.NETStandard/tree/1.5.374.158

OPC Foundation Vulnerability Information

Vulnerabilities and Exposures list:

Vulnerability	CVE number	Publicly disclosed	Exploited
CWE-305: Authentication Bypass by Primary Weakness	CVE-2024-42513	No	No

Mitigating Factors

The vulnerability only exists when the HTTPS endpoints are enabled, and they use a security policy other than None:

Workarounds

Disable all HTTPS endpoints.

Use HTTPS endpoints with a security policy of None.

If application authentication is required, it must be done with the HTTPS certificates. Installations without HTTPS client certificates (either because they are not used or not visible to the OPC UA server) must rely on user authentication for access control.

Acknowledgments

The OPC Foundation thanks Tom Tervoort, from Secura B.V. (https://www.secura.com/) for reporting this issue.

Disclaimer

Revisions

- V1.0 (February 9th, 2025): Bulletin published.