

OPC Foundation Security Bulletin

Security Update for the OPC UA .NET Standard Stack

Published: May 1st, 2022

Version: 1.0

Executive Summary

This security update resolves a vulnerability in the OPC UA .NET Standard Stack that allows a malicious client or server to bypass the application authentication mechanism and allow a connection to an untrusted peer.

This security update has a base score of 6.5 (medium) using the [CVSS v3.1](#) guidelines.

The CVSS vector string is:

AV:N/AC:L/PR:N/UI:N/S:U/C:L/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.	GitHub Commit https://github.com/OPCFoundation/UA-.NETStandard/tree/1.4.368.58
OPCFoundation/UA-.NET-Legacy	
This version or any version after it.	GitHub Commit https://github.com/OPCFoundation/UA-.NET-Legacy/tree/35199e43d46f0eef793cace12baa806838ddba2c

OPC Foundation Vulnerability Information

Vulnerabilities and Exposures list:

Vulnerability	CVE number	Publicly disclosed	Exploited
CWE-303 Incorrect Implementation of Authentication Algorithm.	CVE-2022-29865	Yes	No

Mitigating Factors

Only affects applications running on Windows or MacOS.

Workarounds

Use self-signed Certificates for application authentication.

Move CAs from the trust list to the issuers list and explicitly add each trusted peer into the trust list.

Require user authentication in addition to application authentication.

Acknowledgments

The OPC Foundation recognizes Daan Keuper & Thijs Alkemade from Computest working with Trend Micro Zero Day Initiative for discovering and reporting this issue.

Disclaimer

The information provided in this disclosure is provided "as is" without warranty of any kind. OPC Foundation disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall OPC Foundation or its suppliers be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if OPC Foundation or its suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the foregoing limitation may not apply.

Revisions

- V1.0 (May 1st, 2022): Bulletin published.