

OPC Foundation Security Bulletin

Security Update for the OPC UA .NET Standard Stack

Published: March 10th, 2021

Version: 1.2

Executive Summary

This security update resolves a vulnerability in OPC UA Clients and Servers built with the OPC UA .NET Standard stack that could allow a rogue application to establish a secure connection.

Vendors that incorporate the OPC UA .NET stack into their products must update their products.

This security update has a base score of 4.2 (medium) using the [CVSS v3.1](#) guidelines.

The CVSS vector string is:

CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C/CR:M/IR:M/AR:M/MAV:L/MAC:L/MPR:H/MUI:N/MS:U/MC:L/MI:L/MA:L

Affected Software

The following software has been updated to address the issue:

Download	Release Date	Replacement
UA-.NETStandard Stack		
This version or any version after it.		Commit in GitHub on 2021-01-07 https://github.com/OPCFoundation/UA-.NETStandard/tree/bfa117b7a73217b26d369c75a2b6cb70884469fc NuGet package: https://github.com/OPCFoundation/UA-.NETStandard/releases/tag/1.4.365.10

OPC Foundation Vulnerability Information

CVE-2020-29457

Vulnerabilities and Exposures list:

Vulnerability	CVE number	Publicly disclosed	Exploited
---------------	------------	--------------------	-----------

Rogue application can trick a user into allowing communication.	CVE-2020-29457	No	No
---	--------------------------------	----	----

Mitigating Factors

Applications that do not allow certificate validation errors to be suppressed are not affected.

At least one certificate in the chain needs to be trusted for this exploit to work which means a malicious actor needs write access to the trust list on the server machine.

Workarounds

Do not suppress any certificate errors.

Do not allow users to temporarily trust untrusted application.

Acknowledgments

The OPC Foundation recognizes Thomas Nehring of SAP for discovering this vulnerability.

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 (February 15th, 2021): Bulletin published.
- V1.1 (February 25th, 2021): Clarified that the NuGet package version listed does have the fix.
- V1.2 (March 10th, 2021): Fixed confusing wording.