OPC Foundation Security Bulletin

Security Update for the OPC UA .NET Standard Stack

Published: April 15th, 2020
Version: 1.1

Executive Summary

This security update resolves a vulnerability in OPC UA Servers built with the OPC UA .NET Standard stack that could cause a server to crash when sent malformed messages.

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

This security update is rated 7.5 (high) using the [CVSS v3.1](#) guidelines.

The CVSS vector string is:

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:F/RL:O/RC:C

Affected Software

The following software downloads are affected:

Download	Release Date	Replacement
[UA-.NETStandard Stack and Sample Code](#)		
Any version after date of fix.		Commit in GitHub on 2020-02-18 https://github.com/OPCFoundation/UA-.NETStandard/commit/e606f3aa8ca515ef1432af2be8b0e8697f91dbf2 NuGet package: https://www.nuget.org/packages/OPCFoundation.NetStandard.Opc.Ua/1.4.360.33

OPC Foundation Vulnerability Information

CVE-2020-8867
Vulnerabilities and Exposures list:

Vulnerability	CVE number	Publicly disclosed	Exploited
Malformed messages cause server to crash.	CVE-2020-8867	No	Yes

Mitigating Factors

None.

Workarounds

Enabling security will make exploiting this vulnerability more difficult.

Acknowledgments

The OPC Foundation recognizes Steven Seeley (mr_me) and Chris Anastasio (muffin) working with Trend Micro's 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 (April 15th, 2020): Bulletin published.
- V1.1 (April 15th, 2020): Acknowledgements revised.