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 to cause a server to trigger an out of memory exception with a carefully crafted message.

This security update has a base score of 7.5 (high) using the CVSS v3.1 guidelines.

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

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 Tag 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-789 Memory Allocation with Excessive Size Value.	CVE-2022-29863	No	No

Mitigating Factors

None.

Workarounds

Use a physically secured network where unauthorized clients cannot connect.

Acknowledgments

The OPC Foundation recognizes the Uriya Yavnieli from JFrog Security Research 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.