

OPC Foundation Security Bulletin

Security Update for the OPC UA .NET Standard Reference Server

Published: May 3rd, 2023

Version: 1.0

Executive Summary

This security update resolves a vulnerability in the OPC UA .NET Standard Reference Server that allows remote attackers to send malicious requests that consume all memory available to the server.

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/E:F/RL:O/RC:C](#)

Affected Software

The following software has been updated to address the issue:

Download	Replacement
OPCFoundation/UA-.NETStandard	
This version or any version after it.	Release 1.4.371.86

OPC Foundation Vulnerability Information

Vulnerabilities and Exposures list:

Vulnerability	CVE number	Publicly disclosed	Exploited
CWE-1325 : Improperly Controlled Sequential Memory Allocation	CVE-2023-27321	No	No

Mitigating Factors

None.

Workarounds

None.

Acknowledgments

The OPC Foundation recognizes Claroty Team82 Research 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 3rd, 2023): Bulletin published.