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 expose sensitive information.

This security update has a base score of 5.3 (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:N/A:N/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-209: Generation of Error Message Containing Sensitive Information	CVE-2023-31048	No	No

Mitigating Factors

The information exposed is stack trace information from code that is publicly available. This means the information is less likely to be useful to malicious actors.

Workarounds

None.

Acknowledgments

The OPC Foundation recognizes Sharon Brizinov of Claroty Research – Team82 for discovering and reporting this issue.

Disclaimer

Revisions

- V1.0 (May 3rd, 2023): Bulletin published.