OPC Foundation Security Bulletin

Security Update for the OPC UA .NET Standard Reference Server

Published: August 1st, 2022
Version: 1.0

Executive Summary

This security update resolves a vulnerability in the OPC UA .NET Standard Reference Server that leaks sensitive information to unauthenticated Clients.

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

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 Commit: https://github.com/OPCFoundation/UA-.NETStandard/commit/313aa2a2499d8690cf719a67176e131517bb8b78

OPC Foundation Vulnerability Information

Vulnerabilities and Exposures list:

Vulnerability	CVE number	Publicly disclosed	Exploited
CWE-200: Exposure of Sensitive Information to an Unauthorized Actor	CVE-2022-33916	No	No

Mitigating Factors

None.

Workarounds

Require user and application authentication.

Acknowledgments

The OPC Foundation recognizes Uri Katz of Claroty 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 (August 1st, 2022): Bulletin published.