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:

Affected Software

The following software has been updated to address the issue:

<table>
<thead>
<tr>
<th>Download</th>
<th>Replacement</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://github.com/OPCFoundation/UA-.NETStandard">OPCFoundation/UA-.NETStandard</a></td>
<td>This version or any version after it. Release <a href="https://github.com/OPCFoundation/UA-.NETStandard/releases/tag/1.4.371.86">1.4.371.86</a></td>
</tr>
</tbody>
</table>

OPC Foundation Vulnerability Information

Vulnerabilities and Exposures list:

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>CVE number</th>
<th>Publicly disclosed</th>
<th>Exploited</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://cwe.mitre.org/cwe-209.html">CWE-209</a>: Generation of Error Message Containing Sensitive Information</td>
<td>CVE-2023-31048</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
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

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.