OPC Foundation Security Bulletin

Security Update for the OPC UA .NET Sample Code

Published: July 31st, 2017
Version: 1.0

Executive Summary

This security update resolves a vulnerability in the OPC UA .NET Sample Code and older versions of the Local Discovery Services (LDS) binaries which can be downloaded from the OPC Foundation website. The vulnerability can allow remote attacker to trick the .NET libraries used by the LDS and OPC UA Servers into accessing network resources chosen by the attacker.

Vendors that incorporated the OPC UA .NET Sample Code into their product must update their products.

This security update is rated 8.2 (high) using the CVSS v3.0 guidelines.

The CVSS vector string is:

Affected Software

The following software downloads are affected:

<table>
<thead>
<tr>
<th>Download</th>
<th>Release Date</th>
<th>Replacement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Discovery Server (LDS)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.01.333.0</td>
<td>2011-11-26</td>
<td>1.03.367</td>
</tr>
<tr>
<td>.NET Stack and Sample Applications</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Any version prior to date of fix.</td>
<td>Commit in GitHub on 2017-03-21: <a href="https://github.com/OPCFoundation/UA-.NET/commit/14cb63161897ea3a48400b67bfbcfcb1afec3541">https://github.com/OPCFoundation/UA-.NET/commit/14cb63161897ea3a48400b67bfbcfcb1afec3541</a></td>
<td></td>
</tr>
</tbody>
</table>

OPC Foundation Vulnerability Information
**CVE-2017-12069**

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 remote attacker can trick the .NET libraries used by the LDS and the OPC UA .NET Sample Servers into accessing network resources chosen by the attacker.</td>
<td>CVE-2017-12069</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Mitigating Factors**

The code that accesses the attacker’s URL should ignore any response that is not a valid XML DTD. This means the exploit cannot be used to trigger execution of programs on the target machine, however, it could be used as a denial of service attack.

**Workarounds**

The OPC Foundation has not identified any workarounds for this vulnerability.

**Acknowledgments**

The OPC Foundation recognizes the Siemens and Kaspersky Labs for identifying 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 (July 31\textsuperscript{th}, 2017): Bulletin published.