

OPC Foundation Security Bulletin

Security Update for the OPC UA .NET Sample Code

Published: July 31th, 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:

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H/E:P/RL:O/RC:C/CR:L/IR:L/AR:L/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:N/MI:N/MA:H

Affected Software

The following software downloads are affected:

Download	Release Date	Replacement
Local Discovery Server (LDS)		
1.01.333.0	2011-11-26	1.03.367
.NET Stack and Sample Applications		
Any version prior to date of fix.	Commit in GitHub on 2017-03-21: https://github.com/OPCFoundation/UA-.NET/commit/14cb63161897ea3a48400b67bfbcfdb1afec3541	

OPC Foundation Vulnerability Information

CVE-2017-12069

Vulnerabilities and Exposures list:

Vulnerability	CVE number	Publicly disclosed	Exploited
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.	CVE-2017-12069	No	Yes

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 31th, 2017): Bulletin published.