

OPC Foundation Security Bulletin

Security Update for the OPC UA .NET and Java Client

Published: March 10th, 2020

Version: 1.0

Executive Summary

This security update resolves a vulnerability in OPC UA Clients built with the OPC UA .NET or Java codebases that could result in encrypted password credentials or signed X509 certificate credentials being sent in a form that can be intercepted and reused.

Vendors that incorporate the OPC UA .NET or Java codebase into their client products must update their products.

This security update is rated 7.5 (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:N/I:H/A:N

Affected Software

The following software downloads have updates that address the issue available:

Download	Release Date	Replacement
UA-.NETStandard Stack and Sample Code		
Any version after date of fix.		Commit in GitHub on 2020-01-30: https://github.com/OPCFoundation/UA-.NETStandard/commit/636f5c03f95130ae71880975793e5da7d69591d4 Updated NuGet Packages: 1.4.359.31
UA-.NET-Legacy Stack and Sample Code		
Any version after date of fix.		Commit in GitHub on 2020-01-31: https://github.com/OPCFoundation/UA-.NET-Legacy/commit/04c007865bfe855c65290c5639a70ae0d0f49e2d

UA-Java-Legacy Stack	
Any version after date of fix.	Commit in GitHub on 2020-02-12: https://github.com/OPCFoundation/UA-Java-Legacy/commit/a38aea9266dcbd923fac210bc34c7b41b88bf06e

OPC Foundation Vulnerability Information

CVE-2019-19135

Vulnerabilities and Exposures list:

Vulnerability	CVE number	Publicly disclosed	Exploited
Encrypted user credentials sent to a misbehaving Server can be intercepted and reused by an attacker.	CVE-2019-19135	No	No

Mitigating Factors

The vulnerability only exists if network communication is not encrypted.

The vulnerability only affects Clients communicating with Servers which do not comply with the specification.

Workarounds

Enabling encrypted communication eliminates the risk.

Acknowledgments

The OPC Foundation recognizes Bernd Edlinger at Softing 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 (March 10th, 2020): Bulletin published.