OPC Foundation Security Bulletin

Security Update for the OPC UA Client Applications

Published: September 25th, 2018
Version: 1.0

Executive Summary

This security update resolves a vulnerability in OPC UA client applications that could allow attacker to decrypt passwords sent to an OPC UA Server when the attacker has control over a piece of network infrastructure. The fix requires that OPC UA clients refuse to use untrusted certificates to encrypt data sent to the OPC UA server. This vulnerability only exists when the client uses UserIdentityToken encryption while establishing a Session with SecurityMode None.

Vendors need to review their applications and ensure trusted certificates are used before encrypting any UserIdentityToken.

This security update is rated 5.3 (medium) using the CVSS v3.0 guidelines.

The CVSS vector string is:
CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N/E:U/RL:O/RC:C

Affected Software

The following software downloads provided by the OPC Foundation are affected:

Download	Release Date	Replacement
UA-.NETStandard Stack and Sample Code		
Any version after date of fix.		Commit in GitHub on 2018-07-17. NuGet Packages: Version 1.4.353.15 or later.
UA-.NET-Legacy Stack and Sample Code		
Any version after date of fix.		Commit in GitHub on 2018-07-18.

OPC Foundation Vulnerability Information

CVE-2018-12087

Vulnerabilities and Exposures list:

Vulnerability	CVE number	Publicly disclosed	Exploited
Failure to validate certificates in OPC UA clients communicating without security allow attackers with control over a piece of network infrastructure to decrypt passwords.	CVE-2018-12087	No	No

Mitigating Factors

This attack only affects UserIdentityTokens encrypted when using SecurityMode None.

The attacker requires control over network infrastructure such as a router.

Workarounds

Clients can be configured to not allow the use of the SecurityMode None policy.

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 (September 25th, , 2018): Bulletin published.