OPC Foundation Security Bulletin

Security Update for the OPC UA Stacks

Published: April 12th, 2018
Version: 1.0

Executive Summary

This security update resolves a vulnerability in the OPC UA stacks that can allow remote attacker to exploit a Server's private key by sending carefully constructed UserIdentityTokens encrypted with the Basic128Rsa15 security policy. The update affects client and server applications. This vulnerability could allow an attacker to decrypt passwords even if they are encrypted with another security policy such as Basic256Sha256.

Vendors that incorporated the OPC UA stacks into their product must update their products.

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

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

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 2018-04-12. NuGet Packages: Version 1.3.352.12 or later.
UA-.NET-Legacy Stack and Sample Code		
Any version after date of fix.		Commit in GitHub on 2018-03-13.

OPC Foundation Vulnerability Information

CVE-2018-7559

Vulnerabilities and Exposures list:

Vulnerability	CVE number	Publicly disclosed	Exploited
A remote attacker can use the Server's private key to decrypt and sign messages by using information obtained by sending invalid UserIdentityTokens encrypted with the Basic128Rsa15 security policy. The update affects client and server applications.	CVE-2018-7559	No	Yes

Mitigating Factors

This attack only affects UserIdentityTokens encrypted with the Basic128Rsa15 Security Policy which has already been depreciated.

The Servers can be updated to eliminate the vulnerability even when an unpatched Client connects.

Servers can allow only trusted Client applications and quickly lock applications that have multiple logon failures.

Workarounds

Servers can be configured to not allow the use of the Basic128Rsa15 policy.

Acknowledgments

The OPC Foundation recognizes Bernd Edlinger at Softing for discovering and reporting this issue.

Disclaimer

Revisions

- V1.0 (April 12st, 2018): Bulletin published.