OPC Foundation Security Bulletin

Security Update for the OPC UA Stacks

Published: September 12st, 2018
Version: 1.0

Executive Summary

This security update resolves a vulnerability in OPC UA applications where an attacker trigger could stack overflow by sending carefully structured requests.

Vendors need to ensure their applications use the latest stacks.

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:N/A:H/E:P/RL:O/RC:C/CR:L/IR:L/AR:H/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:N/MI:N/MA:H

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 2018-07-09. 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 2018-07-05.
UA-AnsiC Stack		
Any version after date of fix.		Commit in GitHub on 2017-01-19.
UA-Java Stack		

Any version after date of fix.	Commit in GitHub on 2018-06-06.

OPC Foundation Vulnerability Information

CVE-2018-12086

Vulnerabilities and Exposures list:

Vulnerability	CVE number	Publicly disclosed	Exploited
Buffer overflow in OPC UA applications allows remote attackers to trigger a stack overflow with carefully structured requests.	CVE-2018-12086	No	No

Mitigating Factors

Not applicable.

Workarounds

Not applicable.

Acknowledgments

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

Disclaimer

Revisions

- V1.0 (September 12th, 2018): Bulletin published.