OPC Foundation Security Bulletin

Security Update for the OPC UA Java and .NET Stack

Published: September 12th, 2018
Version: 1.0

Executive Summary

This security update resolves an XXE vulnerability in the OPC UA Java and .NET Legacy Stacks that allowed remote attackers to send carefully constructed requests that caused an OPC UA to access unauthorized sites and potentially causing a denial of service.

Vendors that incorporated the OPC UA Java or .NET Legacy Stack 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
Java Stack		
Any version prior to date of fix.		Commit in GitHub on 2018-06-06.
.NET Legacy Stack		
Any version prior to date of fix.		Commit in GitHub on 2018-07-05.

OPC Foundation Vulnerability Information

CVE-2018-12585

Vulnerabilities and Exposures list:

Vulnerability	CVE number	Publicly disclosed	Exploited
An XXE vulnerability in the OPC UA Java and .NET Legacy Stack can allow remote attackers to trigger a denial of service.	CVE-2018-12585	Yes	No

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 Prosys OPC Ltd 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 (September 12th, 2018): Bulletin published.