OPC Foundation Security Bulletin

Security Update for Autogenerated ANSI C Stack Stubs

Published: March 1st, 2022
Version: 1.0

Executive Summary

This security update resolves a vulnerability in the autogenerated ANSI C stack stubs that allows a malicious server to produce a null pointer error in the client. Any application that uses these stubs is affected including any application based on the OPCFoundation/UA-AnsiC-Legacy codebase.

This security update has a base score of 6.0 (medium) using the CVSS v3.1 guidelines.

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

Affected Software

The following software has been updated to address the issue:

Download	Release Date	Replacement
OPCFoundation/UA-Nodeset		
This version or any version after it.		GitHub Commit d69b75a4b90ed21fbf57a330181f29c75fa2b072. https://github.com/OPCFoundation/UA-NodeSet/commit/d69b75a4b90ed21fbf57a330181f29c75fa2b072

OPC Foundation Vulnerability Information

Vulnerabilities and Exposures list:

Vulnerability	CVE number	Publicly disclosed	Exploited
CWE-476 NULL Pointer Dereference	CVE-2021-45117	No	No

Mitigating Factors

Exploiting this vulnerability requires a client to choose to connect to a malicious server or an attacker who can manipulate packets as they travel across the network.

Workarounds

Do not connect to servers that have been discovered via mDNS, an LDS, an untrusted GDS, or a trusted GDS using SecurityMode=None. Do not call FindServers or GetEndpoints with SecurityMode=None.

Disclaimer

Revisions

- V1.0 (March 1st, 2022): Bulletin published.