Softing Security Bulletin

Security Update for OPC UA C++ SDK

Published: 08.11.2021
Version: 1.0

Executive Summary

This security update resolves a vulnerability in the Softing OPC UA C++ SDK Client Functionality.
Remote attackers may cause a denial of service (DoS) by sending carefully crafted messages.
The client process may crash unexpectedly because of a wrong type-cast and must be restarted.
This security update has a base score of 6.5 (medium) using the CVSS v3.1 guidelines.

The CVSS vector string is:
AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

Affected Software

The following software has been updated to address the issue:

OPC UA C++ SDK - affected: all versions up to 5.65, fixed: 5.66
TH SCOPE – affected: all versions from V3.5, fixed: N. A.
dataFEED OPC Suite – affected: all versions up to 5.17, fixed: 5.18
Secure Integration Server – affected: all versions up to 1.22, fixed: planned for 1.30

The latest version can be downloaded here:
https://industrial.softing.com/support/downloads.html

Softing Vulnerability Information

Vulnerability	CVE Number	Publicly disclosed	Exploited
CWE-20: Improper Input Validation	CVE-2021-40871	No	No

Mitigating Factors

The attack depends on the client to establish a connection to an untrusted and possibly compromised server.

Workarounds

Use a secure connection to avoid communication with untrusted servers.

Disclaimer

The information provided in this disclosure is provided "as is" without warranty of any kind. Softing disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Softing or its suppliers be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Softing 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 (Date TBD): Bulletin published.