Softing Security Bulletin

Security Update for uaToolkit Embedded

Published: 08.11.2021
Version: 1.0

Executive Summary

This security update resolves a vulnerability in the Softing uaToolkit Embedded Server Component. Remote attackers may cause a denial of service (DoS) by sending carefully crafted messages to a OPC/UA server or login as anonymous user, by-passing proper security checks.
The server process may crash unexpectedly because of an invalid type-cast and must be restarted.
This security update has a base score of 7.5 (high) using the CVSS v3.1 guidelines.

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

Affected Software

The following software has been updated to address the issue:

uaToolkit Embedded - affected: all versions up to 1.31, fixed: 1.40
smartLink HW-DP – affected: all versions from 1.10, fixed: planned for 1.19

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-2021-40872	No	No

Mitigating Factors

None.

Workarounds

None.

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.