OPC Foundation Security Bulletin

Security Update for Local Discovery Server (LDS)

Published: Sept 1st, 2021
Version: 1.0

Executive Summary

This security update resolves a vulnerability in the Local Discovery Server (LDS) that allows remote attackers to cause a denial of service (DoS) by sending carefully crafted messages.

This security update has a base score of 7.5 (high) using the CVSS v3.1 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

Affected Software

The following software has been updated to address the issue:

Download	Release Date	Replacement
OPCFoundation/UA-LDS		
This version or any version after it.		1.04.402.463 (Windows Installer) GitHub Commit a0265314fa886437af8c097f220bf670db35e2ac. https://github.com/OPCFoundation/UA-LDS/commit/a0265314fa886437af8c097f220bf670db35e2ac

OPC Foundation Vulnerability Information

Vulnerabilities and Exposures list:

Vulnerability	CVE number	Publicly disclosed	Exploited

CWE-788 Access of Memory Location After End of Buffer	CVE-2021-40142	No	No

Mitigating Factors

The LDS is a non-critical process that can be restarted whenever needed.

Workarounds

Ensure LDS automatically restarts after unexpected failure.

Acknowledgments

Thanks to Bernd Edlinger of Softing for reporting this vulnerability to OPC Foundation.

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 (Sept 1st, 2021): Bulletin published.