

OPC Foundation Security Bulletin

Security Update for Local Discovery Server (LDS)

Published: Nov 17th, 2022

Version: 1.0

Executive Summary

This security update resolves a vulnerability in the Local Discovery Server (LDS) that allows normal user to create a malicious file that is loaded by the LDS running as a high privilege user.

This security update has a base score of 7.8 (high) using the [CVSSv3.1](#) guidelines.

The CVSS vector string is:

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/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.		1.04.405.479 (Windows Installer) GitHub Commit a0265314fa886437af8c097f220bf670db35e2ac. https://github.com/OPCFoundation/UA-LDS/commit/72884edaf8d8ee5a19c07a8913e6b1623d5d96ec

OPC Foundation Vulnerability Information

Vulnerabilities and Exposures list:

Vulnerability	CVE number	Publicly disclosed	Exploited
---------------	------------	--------------------	-----------

CWE-732 : Incorrect Permission Assignment for Critical Resource	CVE-2022-44725	No	No
---	----------------	----	----

Mitigating Factors

Administrators can set file system permissions to block this vulnerability.

Workarounds

Ensure the hardcoded path (C:\Build\Projects\UA-LDS\stack\openss\ssl) to the configuration file exists and can only be accessed by administrators.

Acknowledgments

Thanks to Michael Heinzl 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 (Nov 17th, 2022): Bulletin published.