OPC Foundation Security Bulletin

Security Update for the Local Discovery Server (LDS)

Published: December 6th, 2017
Version: 1.0

Executive Summary

This security update to resolves multiple vulnerabilities that allow an attacker to trigger a crash by placing invalid data into the configuration file. This vulnerability requires an attacker with access to the file system where the configuration file is stored; however, if the configuration file is altered the LDS will be unavailable until it is repaired.

Vendors that distribute the LDS with their products should update their installation with the patched executable. Users that install the LDS manually should download and install the patched version.

This security update is rated 4.4 (Medium) using the CVSS v3.0 guidelines.

The CVSS vector string is:
CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H/E:F/RL:O/RC:C/CR:L/IR:L/AR:L/MAV:L/MAC:L/MPR:H/MUI:N/MS:U/MC:N/MI:N/MA:H

Affected Software

The following software downloads are affected:

Download	Release Date	Replacement
Local Discovery Server (LDS)		
1.03.370	2017-10-07	1.03.371

OPC Foundation Vulnerability Information

CVE-2017-17443

Vulnerabilities and Exposures list:

Vulnerability	CVE number	Publicly disclosed	Exploited

An attacker with access to the LDS configuration file can trigger a crash by placing invalid data into the configuration file.	CVE-2017-17443	No	Yes

Mitigating Factors

The exploit requires access to the file system and permission to change the LDS configuration files.

Workarounds

The OPC Foundation has not identified any workarounds for this vulnerability.

Acknowledgments

The OPC Foundation recognizes Kaspersky Labs for identifying and reporting this issue.

Disclaimer

Revisions

- V1.0 (December 6th, 2017): Bulletin published.