Talos Vulnerability Report

TALOS-2020-1154

LogicalDoc installation privilege escalation vulnerability

NOVEMBER 10, 2020

CVE NUMBER

CVE-2020-13542

Summary

A local privilege elevation vulnerability exists in the file system permissions of LogicalDoc 8.5.1 installation. Depending on the vector chosen, an attacker can either replace the service binary or replace DLL files loaded by the service, both which get executed by a service thus executing arbitrary commands with System privileges.

Tested Versions

LogicalDoc 8.5.1

Product URLs

https://www.logicaldoc.com/product/overview

CVSSv3 Score

9.3 - CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CWE

CWE-276 - Incorrect Default Permissions

Details

LogicalDoc Document Management System is a proprietary document management system designed to handle document storage and indexing using Lucene engine.

By default, LogicalDoc is installed in “C:\LogicalDOC” directory and it allows “Authenticated Users” group to have “Change” privilage over certain files in the directory which are executed with SYSTEM authority. This allows users in any authenticated group to read, write or modify arbitrary files in the install directory resulting in privilage escalation.

The base LogicalDoc directory has lax permissions, providing any auhenticated user with change permissions in the directory:

```
C:\LogicalDOC BUILTIN\Administrators:(OI)(CI)(ID)F
          NT AUTHORITY\SYSTEM:(OI)(CI)(ID)F
          BUILTIN\Users:(OI)(CI)(ID)R
          NT AUTHORITY\Authenticated Users:(ID)C
          NT AUTHORITY\Authenticated Users:(OI)(CI)(IO)(ID)C
```

This allows for several possible attack scenarios:

Any authenticated user on the system to replace binary located in default location as seen below to execute code with privilege of NT SYSTEM user:

```
C:\LogicalDOC\tomcat\bin\LogicalDOC.exe BUILTIN\Administrators:(ID)F
                                        NT AUTHORITY\SYSTEM:(ID)F
                                        BUILTIN\Users:(ID)R
                                        NT AUTHORITY\Authenticated Users:(ID)C
```

They could also replace the update binary, again allowing code execution with NT SYSTEM level privileges:

```
C:\LogicalDOC\update-wd\update-wd.exe BUILTIN\Administrators:(ID)F
                                      NT AUTHORITY\SYSTEM:(ID)F
                                      BUILTIN\Users:(ID)R
                                      NT AUTHORITY\Authenticated Users:(ID)C
```

An attacker could also replace any of the DLLs loaded by these applications.

Timeline

2020-09-16 - Vendor Disclosure

2020-11-03 - Vendor released patch
2020-11-10 - Public Release

CREDIT

Discovered by Yuri Kramarz of Cisco Talos.