Talos Vulnerability Report

TALOS-2020-1009

Leadtools Image Parser Animated Icon Code Execution Vulnerability

JULY 1, 2020

CVE NUMBER

CVE-2020-6089

Summary

An exploitable code execution vulnerability exists in the ANI file format parser of Leadtools 20. A specially crafted ANI file can cause a buffer overflow resulting in remote code execution. An attacker can provide a malicious file to trigger this vulnerability.

Tested Versions

Leadtools 20

Product URLs

https://www.leadtools.com/

CVSSv3 Score

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

CWE

CWE-787 - Out-of-bounds Write

Details

LEADTOOLS is a collection of comprehensive toolkits to integrate document, medical, multimedia, and imaging technologies into desktop, server, tablet, and mobile applications.

The modules analyzed in this vulnerability are below:

```
Loaded symbol image file: C:\LEADTOOLS 20\Bin\CDLL\x64\lfAniX.DLL
Image path: C:\LEADTOOLS 20\Bin\CDLL\x64\lfAniX.DLL
Image name: lfAniX.DLL
Browse all global symbols  functions  data
Timestamp:        Thu Nov  7 17:04:48 2019 (5DC4BF30)
CheckSum:         00021FCB
ImageSize:        0001C000
File version:     20.0.0.1
Product version:  20.0.0.0
File flags:       0 (Mask 3F)
File OS:          40004 NT Win32
```

One toolkit provided by LEADTOOLS is an ANI image parser. This image parser can be hit from a variety of example applications included the Barcode reader and ImageViewer.

When parsing an ANI image, various structures are parsed. The first header is the `ANIH` header which contains the following information:

```
struct ANIH {
    header: ['a', 'n', 'i', 'h'],
    header_size: u32,
    num_frames: u32,
    num_steps: u32,
    width: u32,
    height: u32,
    bit_count: u32,
    num_planes: u32,
    display_rate: u32,
    flags: u32,
}
```

In particular, the ANIH header contains the width in pixels of the image itself. Another header that is parsed by Leadtools is the `RATE` header. This header contains only one value. This value is the display rate for frame 0.

```
struct RATE {
    header: ['r', 'a', 't', 'e'],
    size: u32
}
```

When encountering the `RATE` header, a buffer is allocated based on the provided rate from the image. This buffer is then filled with the number of bytes provided by the width field in the `ANIH` header.

```
LfAniX+0x1578
if ( rate_header.signature == 'etar' )
{
    v10 = L_LocalAllocInit(
            (unsigned int)rate_header.display_rate,
            1i64,
            345i64,
            ...);
    v57 = v10;
    if ( v10 )
        L_RedirectedRead(v6, v10, (unsigned int)(4 * anih_header.width));
}
```

It is possible to provide a display rate such that a small enough buffer is allocated that when it is populated using the provided width value, the allocated buffer is overwritten. This corruption of the heap could potentially result in code execution.

Timeline

2020-02-11 - Vendor Disclosure
2020-06-08 - Talos extended disclosure deadline to 2020-06-30
2020-06-29 - Vendor Patched
2020-07-01 - Public Release

CREDIT

Discovered by Cory Duplantis of Cisco Talos.

VULNERABILITY REPORTS

PREVIOUS REPORT TALOS-2019-0971

NEXT REPORT TALOS-2020-1088