Lexmark Security Advisory:

Revision: 1.1
Last update: 18 August 2016
Public Release Date: 22 August 2016

Summary

Three separate vulnerabilities have been found in Lexmark Perceptive Document Filters that can potentially result in the arbitrary code execution.

References

CVEs: CVE-2016-5646
CVE-2016-4335
CVE-2016-4336

Details

CVE-2016-5646

An exploitable heap overflow vulnerability exists in the Compound Binary Format (CBFF) parser functionality of the Lexmark Perceptive Document Filters Library. An authenticated but malicious User can create a crafted CBFF file to trigger this vulnerability and can cause arbitrary code execution.

CVE-2016-4336

An exploitable out of bounds write vulnerability exists in the Bzip2 parsing of the Perceptive Document Filters conversion functionality. An authenticated but malicious User can create a crafted Bzip2 document to trigger the vulnerability and can lead to a stack based buffer overflow causing an out of bounds write which under the right circumstance could potentially be leveraged to cause arbitrary code execution.

CVE-2016-4335

An exploitable buffer overflow vulnerability exists in the XLS parsing of the Perceptive Document Filters conversion functionality. An authenticated but malicious User can create a crafted XLS document to trigger the vulnerability and can lead to a stack based buffer overflow resulting in arbitrary code execution.

CVSSv3 Scores:

CVE-2016-5646: 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)
CVE-2016-4336: 7.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L)
CVE-2016-4335: 10.0 (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

CVSSv3 scores are calculated in accordance with CVSS version 3.0 (https://www.first.org/cvss/user-guide)

Impact

The vulnerabilities can lead to the execution of arbitrary or potentially malicious code on systems running the affected products

Affected Products

Lexmark Product	Affected Releases	Fixed Releases
Perceptive Document Filters	11.3 and previous	11.3 Build 2228 released 8/8/2016
File Conversion Component	1.5.3 and previous	1.5.4 released 8/15/2016
Perceptive Experience Content Apps (File Conversion Service)	3.0.1 and previous	patch available by 8/31/2016
Perceptive Intelligent Capture	5.6 and 5.7	patch available by ~8/31/2016

Workarounds

Lexmark recommends the following actions:

Perceptive document filters:
Apply patch as described in the patch release documentation.

File Conversion Component:
Apply patch as described in the patch release documentation.

Perceptive Experience Content Apps (File Conversion Service)
Specific file types can be prevented from being rendered by the Perceptive Experience interface, thus avoiding the use of the File conversion Service contained in the app, by adding the vulnerable file types to the "norenditionfiletypes" property in the config.json file. (file types: .xls, .cbff, .BZip2)

See: Perceptive Experience Content Apps (Installation and Setup Guide) page 11 and 12.

Located at:
https://docs.lexmark.com/Experience/en_US/x.x/CA/Print/Perceptive_Experience_Content_Apps_Installation_Guide_x.x.pdf

Apply patch as described in the patch release documentation, when available, and reverse the config.json property settings.

Perceptive Intelligent Capture:
Two workarounds are available for Perceptive Intelligent Capture:

1. Disable CI Document (Coded Information) type in the Perceptive Intelligent Capture Runtime Service Properties. See: Perceptive Intelligent Capture Runtime Server documentation. Located at:

   https://docs.lexmark.com/PIC/en_US/5.7/Runtime_Server/PICRS.htm#Topics/Runtime_Server/Define_document_type.htm%3FTocPath%3DRuntime%250AServer%2520instance%2520configuration%7CConfigure%2520import%2520settings%7C_____2

2. Install the File Server Resource Manager on the Windows Server where the incoming directory is located and configure a File Screen that blocks the copying of the vulnerable file types into the inbound directory configured for Perceptive Intelligent Capture. Apply patch as described in the patch release documentation, when available, and reverse workaround.

Exploitation and Public Announcements

Lexmark is not aware of any malicious use of the vulnerability described in this advisory. The vulnerabilities, identified by Talos, are publicly described at: http://www.talosintelligence.com

Status of this Notice:

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND IS PROVIDED WITHOUT ANY EXPRESS OR IMPLIED GUARANTEE OR WARRANTY WHATSOEVER, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR USE OR PURPOSE.

Distribution

This advisory is posted on Lexmark's web site at http://support.lexmark.com/alerts
Future updates to this document will be posted on Lexmark's web site at the same location.

Revision History

Revision	Date	Reason
1.0	17 August 2016	Initial Draft
1.1	18 August 2016	Grammar changes and Citation