Lexmark Security Advisory:

Revision: 1.0
Last update: 09 December 2016
Public Release Date: 09 December 2016

Summary

Markvision Enterprise contains a vulnerability that allows remote attackers to bypass expected restrictions and load arbitrary classes or access external resources

References

CVE: CVE-2014-0107

Details

Markvision Enterprise is vulnerable to the TransformerFactory bug reported in Apache Xalan-Java. This vulnerability allows remote attackers to bypass expected restrictions and load arbitrary classes or access external resources via a crafted (1) xalan:content-header, (2) xalan:entities, (3) xslt:content-header, or (4) xslt:entities property, or a Java property that is bound to the XSLT 1.0 system-property function.

Impact

Successful exploitation of this vulnerability can lead to bypassing expected restrictions and loading arbitrary classes or accessing external resources.

Vulnerability Scoring Details

CVSSv2 - 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CVSS scores are calculated in accordance with CVSS version 2.0 (https://www.first.org/cvss/v2)

Workarounds

Lexmark recommends updating the application if you have a vulnerable version, but the following workaround can be utilized as a temporary measure.

1. Remove the xalan-2.7.0.jar from the apps/dm-mve/WEB-INF/lib folder in the Markvision Enterprise installation directory.
2. Restart Markvision Enterprise

Software Versions and Fixes

The vulnerability described in this advisory has been fixed in Markvision Enterprise v2.4.2 and all future releases. All releases previous to v2.4.2 are vulnerable.

Obtaining Updated Software

To obtain Markvision Enterprise v2.4.2, please visit http://www.lexmark.com/markvision.

Exploitation and Public Announcements

Lexmark is not aware of any malicious use of the vulnerability described in this advisory.

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	09-December-2016	Initial Public Release