Lexmark Security Advisory:

Revision: 1.1
Last update: 19 July 2021
Public Release Date: 9 December 2014

Summary

Input Validation vulnerability

MarkVision Enterprise contains a vulnerability that allows an unauthenticated remote attacker to download arbitrary files from the MarkVision Enterprise platform.

References

CVE: CVE-2014-8742

Details

MarkVision Enterprise contains a servlet named "ReportDownloadServlet". This servlet allows an unauthenticated remote attacker to download files from arbitrary locations on the MarkVision Enterprise server, including the ability access the authentication credentials for the MarkVision Enterprise database.

Impact

Successful exploitation of this vulnerability can lead to the disclosure of data stored within MarkVision Enterprise.

Vulnerability Scoring Details

CVSS Base Score 7.8
  Impact Subscore: 6.9
  Exploitability Subscore: 10

Exploitability:		Impact:	
Access Vector:	Network	Confidentiality:	Complete
Access Complexity:	Low	Integrity:	None
Authentication:	None	Availability:	None

CVSS scores are calculated in accordance with CVSS version 2.0 (http://www.first.org/cvss/cvss-guide.html)

Workarounds

Lexmark recommends updating the application if you have a vulnerable version.

Please visit http://www.lexmark.com/markvision or contact the Lexmark Technical Support Center at 1-800-539-6275 for additional information.

Software Versions and Fixes

The vulnerability described in this advisory has been fixed in MarkVision Enterprise v2.1 and all future releases. All releases previous to v2.1 are vulnerable.

Obtaining Updated Software

To obtain MarkVision Enterprise v2.1, 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.

Lexmark would like to thank rgod working with HP's Zero Day Initiative (ZDI) for bringing this issue to our attention.

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. LEXMARK RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

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	9-December-2014	Initial Public Release
1.1	19-July-2021	Updated legal notice