Lexmark Security Advisory:

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

Summary

Remote code execution vulnerability

MarkVision Enterprise contains a vulnerability that allows an unauthenticated remote attacker to upload files and execute arbitrary commands with the privilege of the MarkVision Enterprise application.

References

CVE: CVE-2014-8741

Details

MarkVision Enterprise contains a servlet named "GfdFileUploadServerlet". This servlet allows an unauthenticated remote attacker to upload files to arbitrary locations on the MarkVision Enterprise server, including the ability to upload and execute commands with the privilege of the MarkVision Enterprise application.

Impact

Successful exploitation of this vulnerability can lead to the disclosure of data stored in MarkVision Enterprise, and the ability to execute code within the MarkVision platform.

Vulnerability Scoring Details

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

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

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:

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