Lexmark Security Advisory:

Revision: 1.0
Last update: 30 September 2016
Public Release Date: 30 September 2016

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-2016-6918,
Related CVEs: CVE-2015-3269, CVE-2014-8741

Details

During installation Markvision Enterprise (MVE) stores a statically encrypted copy of the user-specified MVE administrator credentials in a text file. These credentials can be extracted by leveraging an AMF vulnerability (CVE-2015-3269). Once extracted the credentials can be decrypted and used to authenticate to the MVE application. Upon authentication, an attacker could leverage a file upload vulnerability (CVE-2014-8741) to upload files to the server hosting MVE which can lead to 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 on the server hosting Markvision Enterprise.

Vulnerability Scoring Details

CVSSv3 Base Score	10.0	(AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)
Impact Subscore:	6.6	
Exploitability Subscore:	3.9	

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

Workarounds

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

The encrypted Markvision Enterprise administrator credential is not updated after installation. Therefore changing the MVE administrator password, after installation is completed, will block access to the CVE-2014-8741 vulnerability. Use the following procedure to change the MVE “admin” password:

1. Log into the MVE web console as the MVE administrator
2. Click on the “Change Password” link at the top right corner of the page.
3. Follow the instructions on changing the password for “admin”
4. Logout of the MVE web console.

Software Versions and Fixes

The vulnerability described in this advisory has been fixed in Markvision Enterprise v2.4.1 and all future releases. All releases previous to v2.4.1 are vulnerable.

Obtaining Updated Software

To obtain Markvision Enterprise v2.4.1, 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 Digital Defense 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.

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	30 September-2016	Initial Public Release