Lexmark Security Advisory:

Revision: 1.0
Last update: 27 April 2018
Public Release Date: 27 April 2018

Summary

Markvision Enterprise (MVE) uses Spring Data REST 2.6.6, which is vulnerable to malicious HTTP PATCH requests and with specially crafted JSON data will run arbitrary Java code.

References

CVE: CVE-2017-8046

Details

MVE is split into two web applications executing in the same tomcat process. The mve-data-service web application, accessible only by localhost clients, is a Spring Boot application that is using a vulnerable version of Spring Data REST and supports HTTP PATCH requests.

Impact

Clients residing on the same host as MVE can submit specially crafted JSON data to mve-data-service that will run arbitrary Java code.

Vulnerability Scoring Details

CVSS v3 Base Score: 6.7 Medium
Vector String: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
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.

Software Versions and Fixes

The vulnerability described in this advisory has been fixed in Markvision Enterprise v3.2 and all future releases. All releases between v3.0 and v3.1.3 are vulnerable.

Obtaining Updated Software

To obtain Markvision Enterprise v3.2, 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	27 April 2018	Initial Public Release