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 cause a denial of service.

References

CVE:	CVE-2016-3092

Details

Markvision Enterprise is vulnerable to the MultipartStream bug reported in the Apache Commons Fileupload library. This vulnerability allows remote attackers to cause a denial of service (CPU consumption) via a long boundary string.

Impact

Successful exploitation of this vulnerability can lead to a denial of service.

Vulnerability Scoring Details

CVSSv2 - 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CVSSv2 scores are calculated in accordance with CVSS version 2.0 (https://www.first.org/cvss/v2)

CVSSv3 - 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
CVSSv3 scores are calculated in accordance with CVSS version 3.0 (https://www.first.org/cvss)

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 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