Lexmark Security Advisory:

Revision: 1.0
Last update: 28 August 2018
Public Release Date: 28 August 2018

Summary

Markvision Enterprise (MVE) uses Apache Tomcat which is vulnerable to a bug that could allow an attacker to cause MVE to enter an infiniite loop and produce a denial of service condition.

References

CVE: CVE-2018-1336

Details

MVE uses a vulnerable version of Apache Tomcat for hosting the MVE web application. Due to an overflow vulnerability in the UTF-8 decoder, improper handling of input characters can result in an infinite loop and produce a denial of service condition.

Impact

An attacker could deny service to users of the MVE application.

Vulnerability Scoring Details

CVSS v3 Base Score: 7.5
Vector String: CVSS:3.0/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/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 v3.3 and all future releases. All releases between v2.2.0 and 3.2.1 are vulnerable.

Obtaining Updated Software

To obtain Markvision Enterprise v3.3, 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	28 August 2018	Initial Public Release