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 an information disclosure bug that could allow an attacker to reuse session credentials from a previous user's session in a new session.

References

CVE: CVE-2018-8037

Details

MVE uses a vulnerable version of Apache Tomcat for hosting the MVE web application. The Apache Tomcat HTTP connectors have a flaw in connection handling that could allow an attacker to submit malicious input and access sensitive session credentials by receiving the response from a different user.

Impact

An attacker could obtain a previous user's session credentials and pose as that user in a new session.

Vulnerability Scoring Details

CVSS v3 Base Score: 9.1
Vector String: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
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 v3.0 and 3.2.1 inclusive 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