Lexmark Security Advisory:

Revision: 1.0
Last update: 9 March 2018
Public Release Date: 9 March 2018

Summary

Markvision Enterprise contains a vulnerability when configured to use TLS binding for LDAP that allows clients to logon with a valid username and any arbitrary password.

References

CVE: CVE-2017-8028

Details

Markvision Enterprise uses the Pivotal Spring-LDAP library for connecting to LDAP servers for authentication. When an administrator checks the Enable LDAP for authentication option and chooses TLS as the binding type Markvision Enterprise will authenticate users without validating the entered password. Therefore, anyone who knows a valid username can access the system with the roles of that user.

Impact

An attacker who exploits this vulnerability can gain access to all the data in MVE and can run any tasks allowed by the user's role.

Vulnerability Scoring Details

CVSS v3 Base Score: 9.4   Critical
Vector String: CVSS**:**3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L
CVSSv3 scores are calculated in accordance with CVSS version 3.0 (https://www.first.org/cvss/user-guide)

Workarounds

Lexmark recommends either disabling LDAP authentication or using a non-vulnerable binding type such as Kerberos or Simple if it is not possible to upgrade to Markvision v3.1.3.

Software Versions and Fixes

The vulnerability described in this advisory has been fixed in Markvision Enterprise v3.1.3 and all future releases. Only v3.1 and v3.1.2 are vulnerable. All previous versions are not vulnerable.

Obtaining Updated Software

To obtain Markvision Enterprise v3.1.3, 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	9 March 2018	Initial Public Release