Lexmark Security Advisory:

Revision: 1.0
Last update: 28 January 2019
Public Release Date: 28 January 2019

Summary

Credentials to external LDAP and SMTP servers stored in Lexmark devices can be extracted by the device administrator.

References

CVE: CVE-2018-17944

Details

Access credentials to LDAP or SMTP servers are stored in Lexmark devices are not cleared when related settings are changed by the administrator. A malicious administrator can extract these credentials by changing server settings such as the hostname or IP address of the LDAP or SMTP server then initiating an action that causes the Lexmark device to attempt to authenticate. This will cause the Lexmark device to communicate the access credentials to a device controlled by the malicious administrator.

CVSSv3 Base Score	2.7	(AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N)
Impact Subscore:	1.4	
Exploitability Subscore:	1.2	

CVSSv3 scores are calculated in accordance with CVSS version 3.0 (https://www.first.org/cvss/user-guide)

Impact

Successful exploitation of this vulnerability can lead to the disclosure of credentials stored in the device used to access external resources.

Affected Products

All Lexmark devices that support LDAP authentication and email functionality are affected.

Workarounds

Lexmark recommends the following:

1. Devices be configured that access to the settings menus is restricted to trusted administrators.
2. Use LDAP+GSSAPI (Kerberos) when it is supported by the server.
3. Require the use of TLS when it is supported by the server.
4. That LDAP & SMTP account credentials stored in the device follow the practice of least privilege. These accounts should be restricted to only support the following functionality
   SMTP - Email forwarding/delivery

LDAP – Login & read access.

Exploitation and Public Announcements

Lexmark is not aware of any malicious use against Lexmark products of the vulnerability described in this advisory.

Lexmark would like to thank Ramnath Shenoy of Content Security for bringing this to our attention.

Status of this Notice:

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 January 2019	Initial Public Release