Lexmark Security Advisory:

Revision: 1.1
Last update: 8 September 2017
Public Release Date: 13 September 2017

Summary

Orpheus' Lyre Vulnerability
Some older Lexmark products may have a vulnerability that allow attackers to bypass certain security restrictions and perform unauthorized actions by conducting a man-in-the-middle attack.

References

CVE: CVE-2017-11103

Details

Heimdal (an implementation of Kerberos 5) before release 7.4 allows remote attackers to impersonate services with Orpheus' Lyre attacks because it obtains service-principal names in a way that violates the Kerberos 5 protocol specification. In _krb5_extract_ticket() the KDC-REP service name must be obtained from the encrypted version stored in 'enc_part' instead of the unencrypted version stored in 'ticket'. Use of the unencrypted version stored in 'ticket' provides an opportunity for successful server impersonation and other attacks.

NOTE: This CVE is only for Heimdal and other products that embed Heimdal code; it does not apply to other instances in which this part of the Kerberos 5 protocol specification is violated.

CVSS v3 Base Score: 8.1 High (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)
Impact Score: 5.9
Exploitability Score: 2.2

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

Impact

This vulnerability can lead to the unauthorized disclosure of configuration information and user data on the affected device.

Affected Products

To determine a devices firmware level, select the Settings > Reports > Menu Setting Page menu item from the operator panel. If the firmware level listed under "Device Information" matches any level under "Affected Releases", then upgrade to a "Fixed Release".

<table>
<thead>
<tr>
<th>Lexmark Models</th>
<th>Affected Releases</th>
<th>Fixed Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>C746</td>
<td>LHS42.xx.P596 and previous</td>
<td>LHS42.xx.P597 and later</td>
</tr>
<tr>
<td>C748 &amp; CS748</td>
<td>LHS42.xx.P596 and previous</td>
<td>LHS42.xx.P597 and later</td>
</tr>
</tbody>
</table>
### Obtaining Updated Software
To obtain firmware that resolves this issue, or if you have special code, please contact Lexmark's Technical Support Center at [http://support.lexmark.com](http://support.lexmark.com) to find your local support center.

### Recommendations and/or Workarounds
Lexmark recommends updating firmware to address this issue.

### Exploitation and Public Announcements
Lexmark is not aware of any malicious use against Lexmark products 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

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>21 August 2017</td>
<td>Initial Public Release</td>
</tr>
<tr>
<td>1.1</td>
<td>6 September 2017</td>
<td>Included release for LR.xx.P754 and LP.xx.P753</td>
</tr>
</tbody>
</table>