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".

Lexmark Models	Affected Releases	Fixed Release
C746	LHS42.xx.P596 and previous	LHS42.xx.P597 and later
C748 & CS748	LHS42.xx.P596 and previous	LHS42.xx.P597 and later

C79x & CS796	LHS42.xx.P596 and previous	LHS42.xx.P597 and later
C925	LHS42.xx.P596 and previous	LHS42.xx.P597 and later
C95x	LHS42.xx.P596 and previous	LHS42.xx.P597 and later
X548 & XS548	LHS42.xx.P596 and previous	LHS42.xx.P597 and later
X74x & XS748	LHS42.xx.P596 and previous	LHS42.xx.P597 and later
X792 & XS79x	LHS42.xx.P596 and previous	LHS42.xx.P597 and later
X925 & XS925	LHS42.xx.P596 and previous	LHS42.xx.P597 and later
X95x & XS95x	LHS42.xx.P596 and previous	LHS42.xx.P597 and later
E46x & 3330dn	LR.xx.P753 and previous	LR.xx.P754 and later
X46x & 3333dn/ 3335dn	LR.xx.P753 and previous	LR.xx.P754 and later
X65x & 5535dn	LR.xx.P753 and previous	LR.xx.P754 and later
X73x	LR.xx.P753 and previous	LR.xx.P754 and later
T650/T652 & 5230dn/5350dn	LR.xx.P753 and previous	LR.xx.P754 and later
T654 & 5330dn	LR.xx.P753 and previous	LR.xx.P754 and later
C73x	LR.xx.P753 and previous	LR.xx.P754 and later
X86x	LP.xx.P752 and previous	LP.xx.P753 and later
W85x	LP.xx.P752 and previous	LP.xx.P753 and later

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 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:

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	21 August 2017	Initial Public Release
1.1	6 September 2017	Included release for LR.xx.P754 and LP.xx.P753