Lexmark Security Advisory:

Revision: 1.1
Last update: 19 July 2021
Public Release Date: 2 October 2014

Summary

Bash Shellshock Vulnerability

Lexmark has learned of a series of vulnerabilities in the open-source bash shell program that allows an attacker to execute arbitrary commands on a vulnerable system.

No Lexmark devices or software products are affected by this vulnerability.

References

CVE: CVE-2014-6271, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187

Details

On September 24th, 2014 a series of vulnerabilities, commonly referred to as "Shellshock" was announced in the open-source software package bash. The vulnerability allows for arbitrary code execution on affected systems.

Vulnerability Scoring Details (CVE-2014-6271)

CVSS Base Score 10
Impact Subscore: 10
Exploitability Subscore: 10

Exploitability:		Impact:	
Access Vector:	Network	Confidentiality:	Complete
Access Complexity:	Low	Integrity:	Complete
Authentication:	None	Availability:	Complete

CVSS scores are calculated in accordance with CVSS version 2.0 (http://www.first.org/cvss/cvss-guide.html)

Impact

No Lexmark devices or software products are affected by this vulnerability. But customers should confirm that bash is patched for this issue on any system on which Lexmark software is installed.

Unaffected Products

Lexmark devices and software products are not affected by this vulnerability.

Affected Products

No Lexmark devices or software products are affected by this vulnerability.

Exploitation and Public Announcements

Lexmark is aware of unconfirmed reports of 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. LEXMARK RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

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	30 -September-2014	Initial Public Release
1.1	19-July-2021	Updated legal notice