Xerox Security Bulletin XRX15-002

glibc “Ghost” Vulnerability

v1.0
02/09/15

Background

A vulnerability has been discovered in the glibc library software that interacts with the Domain Name System (DNS) that can allow attackers to remotely execute malicious code on a target system. A patch was issued two years ago but most Linux versions used in production systems remained unprotected. Patching requires a system restart so some servers may remain vulnerable for some time to come.

It is noted that this vulnerability is extremely difficult to exploit and so far only one application, Exim (a mail transfer agent), has been shown to be exploitable. It’s possible others may be identified, however. Exploit code for Exim has not yet been published but is expected to be in the future. Although many network-facing applications screen URLs prior to using them, patching the glibc library is still recommended. Please also note that no Xerox device contains the Exim mail transfer agent and it is not possible to install it on a Xerox device.

A set of software patches will be provided to address this vulnerability for affected Xerox products. These software patches are intended for installation by customers. Installation instructions for these software patches will be provided in future versions of this bulletin.

In addition, a glibc “Ghost” vulnerability document addressing this vulnerability has been posted to the URL www.xerox.com/security. This document includes a list of Xerox devices and whether they are or are not vulnerable to this vulnerability or are still under investigation. Future versions of this document will provide estimated availability dates for the software patches for the various affected Xerox products. You may access the document from the URL by clicking on “Learn more” on the main page under the “The Ghost Vulnerability Affects Linux Systems” heading. It requires Adobe Reader or other PDF reader to view.

The glibc “Ghost” vulnerability document and this bulletin will be updated as more detailed information becomes available. You may need to clear your browser cache in order for the new version to be available to you.

Disclaimer

The information provided in this Xerox Product Response is provided "as is" without warranty of any kind. Xerox Corporation disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Xerox Corporation be liable for any damages whatsoever resulting from user's use or disregard of the information provided in this Xerox Product Response including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Xerox Corporation has been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential damages so the foregoing limitation may not apply.

The information in this bulletin is subject to change without notice.