Xerox Product Security

The glibc (Ghost) Vulnerability

Version 3.0

June 1, 2015

Disclaimer

The information provided in this document 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 document 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.

Table of Contents

Introduction

A vulnerability has been discovered in the glibc software in the versions shown below. It allows a heap-based buffer overflow in the **__nss_hostname_digits_dots** function in glibc 2.2, and other 2.x versions before 2.18, allows context-dependent attackers to execute arbitrary code via vectors related to the (1) **gethostbyname** or (2) **gethostbyname2** function, aka "GHOST."

Vulnerable glibc Versions

2.2.5
2.2.4
2.2.3
2.2.2
2.2.1
2.0
2.0.1
2.0.2
2.0.3
2.0.4
2.0.5
2.0.6
2.1
2.1.1
2.1.1.6
2.1.2
2.1.3
2.1.9
2.10.1
2.11
2.11.1
2.11.2
2.11.3
2.12
2.12.1
2.12.2
2.13
2.14
2.14.1
2.15
2.16
2.17
2.2

This problem affects devices that run UNIX and Linux and use glibc . Linux clients or server versions are able to upgrade to a non-vulnerable glibc easily using the APT or RPM Package Management tools. To upgrade a Xerox device or software, a non-vulnerable version of glibc must replace the vulnerable version in a new build of Xerox software and the resultant software must then be installed on each device or application.

This document lists Xerox products and whether they are affected by this issue. For complete details about the vulnerability from the National Vulnerability Database, use this link: http://nvd.nist.gov/nvd.cfm?cvename=CVE-2015-0235

An Important Point

This document contains products that Xerox currently sells and some that they have recently stopped selling. Some of these older products may be vulnerable but a patch may not be made available. This is based entirely on the age of the product and customers with these older products should contact Xerox to discuss options.

Legend for Product Tables

A description of the label in the Affected column is provided below. Dates are estimated and may change over time.

Type of Product	Affected	Meaning
Product Name	**No**	**Product Not Affected by Vulnerability**
Product Name	**Yes**	**Product Affected by Vulnerability**
Product Name	**UI**	**Product Under Investigation**
Product Name	**Details**	**Product Requires More Details**

Monochrome Models	Affected	Patch Availability Date
Phaser® 3010/3040	**No**	**N/A**
Phaser® 3155/3160	**No**	**N/A**
Phaser® 3250	**No**	**N/A**
Phaser® 3320	**No**	**N/A**
Phaser® 3610	**No**	**N/A**
Phaser® 3635 MFP	**No**	**N/A**
Phaser® 4510	**No**	**N/A**
Phaser® 4600/4620	**No**	**N/A**
Phaser® 5335	**No**	**N/A**
Phaser® 5550	**No**	**N/A**
Phaser® 6125	**No**	**N/A**
WorkCentre® 3210/3220	**No**	**N/A**
WorkCentre® 3315/3325	**No**	**N/A**
WorkCentre® 3045 B/NI	**No**	**N/A**
WorkCentre 3550	**No**	**N/A**
WorkCentre® 3615	**No**	**N/A**
WorkCentre® 3655 ConnectKey Technology **Patch available here.**	**Fixed**	**NOW**
WorkCentre® 4150	**No**	**N/A**
WorkCentre® 4250/4260	**No**	**N/A**
WorkCentre® 5135/5150 - **Patch available here.**	**No**	**N/A**
WorkCentre® 5325/5330/5335	**No**	**N/A**
WorkCentre® 5632/5638//5645/5655/5665/5675/5687 **Single Board Patch available here.** WorkCentre® 5632/5638/5645/5655/5665/5675/5687 **Multi-Board Patch available here.**	**Fixed**	**NOW**
WorkCentre® 5735/5740/5745/5755/5765/5775/5790.-. **Software Patch available here.** Release Notes **available here.**	Yes*	**NOW**
WorkCentre® 5845/5855/5865/5875/5890 ConnectKey Technology **Patch available here.**	**Fixed**	**NOW**
WorkCentre® 5945/5955 ConnectKey Technology	Yes*	**3/20/2015**
Xerox® D95/D110/D125/D136® Copier/Printer	**No**	**N/A**
DocuPrint® 425/850, 500/1000, 525/1050CF	**No**	**N/A**
Xerox 495CF	**No**	**N/A**
Xerox 650/1300CF	**No**	**N/A**

* Recommended Actions

1. If your Xerox printer or multifunction has **Yes*** in the **Affected** column, the steps below indicate what you should do to protect yourself against the **glibc** vulnerability.
2. Determine if your Xerox device is networked. If your device is not connected to a network, exploiting this vulnerability is not possible.
3. If possible, upgrade all Linux and UNIX clients and servers that print to a Xerox device. As soon as upgraded software is released, upgrade all your Xerox devices as well.
4. If it is not possible to upgrade all clients, you may wish to have them not communicate with a vulnerable Xerox device or disconnect them from the network until upgraded software is available.
5. Monitor http://www.xerox.com/information-security/ for information regarding an update for your device. Additional instructions will be provided on how to install this update and some additional steps you will need to take once the upgrade is installed.

Color Product Table

Color Models	Affected	Patch Availability Date
Phaser® 6000/6010	No	N/A
Phaser® 6128/6128MFP	No	N/A
Phaser® 6130 Phaser® 6140	No	N/A
Phaser® 6180/6180MFP Phaser® 6280	No	N/A
Phaser® 6360	No	N/A
Phaser® 6500	No	N/A
Phaser® 6600	No	N/A
Phaser® 6700 **Patch available here.**	Fixed	NOW
Phaser® 7100	No	N/A
Phaser® 7400	No	N/A
Phaser® 7500	No	N/A
Phaser® 7800 **Patch available here.**	Fixed	NOW
Phaser® 8560/8560MFP	No	N/A
ColorQube® 8570/8870	No	N/A
ColorQube® 8700/8900 ConnectKey Technology **Patch available here.**	Fixed	NOW
ColorQube® 9201/9202/9203	Yes*	3/20/2015
ColorQube® 9301/9302/9303 ConnectKey Technology **Patch available here.**	Fixed	NOW
WorkCentre® 6015 N/NI	No	N/A
WorkCentre® 6505, WorkCentre® 6605	No	N/A
WorkCentre® 3550	No	N/A
WorkCentre® 6400 **Patch available here.**	Fixed	NOW
WorkCentre® 6655 ConnectKey Technology **Patch available here.**	Fixed	NOW
WorkCentre® 7120/7225	No	N/A
WorkCentre® 7220/7225 ConnectKey Technology **Patch available here.**	Fixed	NOW
WorkCentre® 7328/7335/7345/7346	No	N/A
WorkCentre® 7425/7428/7435	No	N/A
WorkCentre® 7525/7530/7535.7545/7556 **Patch available here.**	Fixed	NOW
WorkCentre® 7655/7665/7675	Yes*	3/20/2015
WorkCentre® 7755/7765/7775	Yes*	3/20/2015
WorkCentre® 7970 ConnectKey **Patch available here.**	Fixed	NOW
WorkCentre® 7830/7835 ConnectKey **Patch available here.**	Fixed	NOW
WorkCentre® 7845/7855 ConnectKey **Patch available here.**	Fixed	NOW
Xerox Color 550/560/570®	No	N/A
Xerox Color C75/J75 Press®	No	N/A

* Recommended Actions

1. If your Xerox printer or multifunction has **Yes*** in the **Affected** column, the steps below indicate what you should do to protect yourself against the **glibc** vulnerability.
2. Determine if your Xerox device is networked. If your device is not connected to a network, exploiting this vulnerability is not possible.
3. If possible, upgrade all Linux and UNIX clients and servers that print to a Xerox device. As soon as upgraded software is released, upgrade all your Xerox devices as well.
4. If it is not possible to upgrade all clients, you may wish to have them not communicate with a vulnerable Xerox device or disconnect them from the network until upgraded software is available.
5. Monitor http://www.xerox.com/information-security/ for information regarding an update for your device. Additional instructions will be provided on how to install this update and some additional steps you will need to take once the upgrade is installed.