Xerox® Product Security

The Shellshock Bash Vulnerability

Version 1.5
October 27, 2014

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 Bash command shell that can allow attackers to remotely execute commands on a target system. Even systems that don't allow remote command shell connections may still use Bash to execute commands in the Apache web server and other network-facing applications. Unix and Unix-derived systems like Linux and Mac OS X are vulnerable to these attacks since they use Bash as the default command shell.

The vulnerability was reported September of 2014 but has been determined to have existed for at least 22 years in various versions of Bash. Therefore, it is likely any currently running system that uses Bash is vulnerable.

The only known solution for this vulnerability is to replace your current version of Bash with a fixed version. If you have a Unix, Linux, Mac OS X or Solaris system, see below for information. Microsoft Windows (all versions, client or servers) is generally not affected, but it may be if software has been installed that includes a Windows version of bash, such as Cygwin.

- Apple Macintosh users (all versions, clients or servers) are not vulnerable by default but some users, particularly software developers, may have made changes to their system that may make them vulnerable. Apple has a patch for Bash for these users to install at http://support.apple.com/kb/HT6495.
- Linux clients or server versions are able to upgrade to a non-vulnerable Bash version easily using the APT or RPM Package Management tools.
- Solaris client or server versions are able to upgrade to a non-vulnerable Bash version easily using the dpkg Package Management tool.
- If you are using the Cygwin version of Bash on Microsoft Windows, update your Bash version using the updater.

Equipment Not Listed Below

Xerox strives to make the list as complete as possible but omissions may occur. If you have a Xerox device that is not listed below and is currently supported by Xerox, please click on Submit a question, report a vulnerability, or request more information on product security under Contact Information on www.xerox.com/security to request information on your device.

Legend for Product Tables

A third column with the explanations is provided below. For the remainder of the document, each table has only two columns.

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**

Hardware Products

Monochrome Product Table

Xerox® Monochrome Product Models	Affected	Estimated Patch Availability
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® 4600/4620/4622	No	N/A
Phaser® 5335	No	N/A
Phaser® 5550	No	N/A
WorkCentre® 3210/3220	No	N/A
WorkCentre® 3315/3325	No	N/A
Phaser® 3635MFP	No	N/A
WorkCentre® 3045 B/NI	No	N/A
WorkCentre® 3550	No	N/A
WorkCentre® 3655	Yes	10/17/2014[1]
WorkCentre® 3615	No	N/A
WorkCentre® 4118	No	N/A
WorkCentre® 4150	No	N/A
WorkCentre® 4250/4260	No	N/A
WorkCentre® 5030/5050	Yes	11/07/2014[2]
WorkCentre® 5135/5150	Yes	10/31/2014[2]
WorkCentre® 5222/5225/5230	No	N/A
WorkCentre® 5325/5330/5335	No	N/A
WorkCentre® 5632/5638/5645/5655/5665/5675/5687	Yes	10/31/2014[2]
WorkCentre® 5740/5745/5755/5765/5775/5790	Yes	10/31/2014[2]
WorkCentre® 5845/5855/5865/5875/5890	Yes	10/17/2014[1]
WorkCentre® 5945/5955	Yes	10/17/2014[1]
WorkCentre® Pro 232/238/245/255/265/275	Yes	11/07/2014[2]
WorkCentre® Bookmark 40/55	Yes	11/07/2014[2]
Xerox® D95/D110/D125 Copier/Printer	No	N/A
Xerox® D136 Copier/Printer and Printer	No	N/A
Xerox® 4590/4595 Digital Copier/Printer	No	N/A
Xerox M20i	No	N/A
DocuPrint® 425/850, 500/1000, 525/1050CF	No	N/A

Xerox® 4112™/4127™ C/P And Enterprise Printing System	No	N/A
Xerox® 495® CF	No	N/A
Xerox® 650/1300® CF	No	N/A
Nuvera All Models	Yes	NOW

[1]Recommended Actions

A. Patch for applicable software system versions '.071.xxx.yyy.xzzzz': SSConnectKey.071v2.zip http://www.xerox.com/downloads/usa/en/s/SSConnectKey.071v2.zip

B. Patch for software system versions '.072.xxx.yyy.xzzzz': SSConnectKey.072v2.zip http://www.xerox.com/downloads/usa/en/s/SSConnectKey.072v2.zip

[2]Recommended Actions

Monitor http://www.xerox.com/security for information regarding an update for your device. Additional instructions will be provided on how to install this update and any additional steps you will need to take once the update is installed.

Color Product Table

Xerox® Color Product Models	Affected	Estimated Patch Availability
DocuColor 8000	No	N/A
Phaser® 6000/6010	No	N/A
Phaser® 6015	No	N/A
Phaser® 6125	No	N/A
Phaser® 6128/6128MFP	No	N/A
Phaser® 6130	No	N/A
Phaser® 6140	No	N/A
Phaser® 6180/6180MFP	No	N/A
Phaser® 6280	No	N/A
Phaser® 6360	No	N/A
Phaser® 6500	No	N/A
Phaser® 6600	No	N/A
Phaser® 6700	Yes	11/07/2014[2]
Phaser® 7100	No	N/A
Phaser® 7400	No	N/A
Phaser® 7500	No	N/A
Phaser® 7800	Yes	11/07/2014[2]
Phaser® 8560/8560MFP	No	N/A
ColorQube® 8570/8870	No	N/A
ColorQube® 8700/8900 Xerox® Built on ConnectKey® Technology	Yes	10/17/2014[1]
ColorQube® 8700/8900	Yes	10/31/2014[2]
ColorQube® 9201/9202/9203	Yes	10/31/2014[2]
ColorQube® 9301/9302/9303	Yes	10/28/2014[2]
ColorQube® 9301/9302/9303 Xerox® Built on ConnectKey® Technology	Yes	10/28/2014[1]
WorkCentre® 3550	No	N/A
WorkCentre® 6015 N/NI	No	N/A
WorkCentre® 6505	No	N/A
WorkCentre® 6605	No	N/A

WorkCentre® 6655	Yes	10/17/2014[1]
WorkCentre® 6400	Yes	10/31/2014[2]
WorkCentre® 7120/7125	No	N/A
WorkCentre® 7220/7225	Yes	10/17/2014[1]
WorkCentre® 7328/7335/7345/7346	No	N/A
WorkCentre® 7425/7428/7435	No	N/A
WorkCentre® 7525/7530/7535/7545/7556	Yes	10/28/2014[2]
WorkCentre® 7655/7665/7675	Yes	11/07/2014[2]
WorkCentre® 7755/7765/7775	Yes	10/31/2014[2]
WorkCentre® 7830/7835/7845/7855	Yes	10/17/2014[1]
WorkCentre® 7970	Yes	10/17/2014[1]
Xerox® Color 550/560/570	No	N/A
Xerox® Color C75®/J75 Press	No	N/A
Xerox® Wide Format IJP 2000	Yes	11/17/2014[2]
Xerox® Wide Format 6705 System	Yes	TBD[2]
Xerox® 490/980® CF	Yes	TBD[2]
Xerox Wide Format 721p ACCXES Controller	No	N/A

[1]Recommended Actions

A. Patch for applicable software system versions '.071.xxx.yyy.xzzzz': SSConnectKey.071v2.zip http://www.xerox.com/downloads/usa/en/s/SSConnectKey.071v2.zip

B. Patch for software system versions '.072.xxx.yyy.xzzzz': SSConnectKey.072v2.zip http://www.xerox.com/downloads/usa/en/s/SSConnectKey.072v2.zip

C. Patch for software system versions '.061.xxx.yyy.xzzzz': SSCQ93xx.061v1.zip: http://www.xerox.com/downloads/usa/en/s/SSCQ93xx.061v1.zip

D. Patch for software system versions '.WorkCentre 75XX all releases: http://www.xerox.com/downloads/usa/en/s/SSWC75xxv1.zip

[2]Recommended Actions

A. Monitor http://www.xerox.com/security for information regarding an update for your device. Additional instructions will be provided on how to install this update and any additional steps you will need to take once the update is installed.

Xerox® FreeFlow® Print Server Table

FreeFlow® Print Server Software	Affected	Patch Availability
FreeFlow® Print Server Version 6.X	Yes	Now[3]
FreeFlow® Print Server Versions 7.X, 8.X and 9.X	Yes	Now[3]
DocuSP® Print Server Version 5.X	Yes	Now[3]

[3]Recommended Actions

A. Please contact your Xerox® representative to have this patch installed.