

Xerox Product Response to CERT[®] Advisory CA-2002-18: *OpenSSH Vulnerabilities in Challenge Response Handling*

Audience and Purpose

The primary audience for this document is Xerox analysts and customers who want information regarding how Xerox products respond to [CERT[®] Advisory CA-2002-18](#), issued by CERT[®] on June 26th, 2002. The following sections provide excerpts from the CERT[®] advisory and the corresponding Xerox response.

Background

The CERT[®] Coordination Center (CERT/CC) is a center of Internet security expertise at the [Software Engineering Institute](#), a federally funded research and development center operated by [Carnegie Mellon University](#). CERT[®] studies Internet security vulnerabilities, handles computer security incidents, publishes security alerts, researches long-term changes in networked systems, and develops information and training to help you improve security at your site.

[CERT[®] Advisory CA-2002-18](#) refers to two related vulnerabilities in the challenge response handling code in OpenSSH versions 2.3.1p1 through 3.3. The vulnerabilities may allow a remote intruder to execute arbitrary code as the user running sshd (often root). The first vulnerability affects OpenSSH versions 2.9.9 through 3.3 that have the challenge response option enabled and that use SKEY or BSD_AUTH authentication. The second vulnerability affects PAM modules using interactive keyboard authentication in OpenSSH versions 2.3.1p1 through 3.3, regardless of the challenge response option setting. Additionally, a number of other possible security problems have been corrected in OpenSSH version 3.4.

Xerox Product Response

The table below lists various products and their positions with respect to [CERT[®] Advisory CA-2002-18](#). This document will be updated with additional product information as it becomes available.

Product	Response to CERT[®] Advisory CA-2002-18
DigiPath	DigiPath does not use OpenSSH and is not, therefore, affected by this vulnerability.
DocuColor 1632/2240	The DocuColor 1632/2240 products are not affected by this vulnerability.
DocuColor 3535 with EFI Network Controller	The DocuColor 3535 with EFI Network Controller does not run SSH and is not, therefore, affected by this vulnerability.
DocuColor Windows NT based products with EFI front-ends: <ul style="list-style-type: none"> • DocuColor 12 with X12 • DocuColor 12 with EX12 • DocuColor 12 with XP12 • DocuColor 2045/2060 with EX2000 • DocuColor 2045/2060 with EX2000d • DocuColor 2045/2060 with EX2000v • DocuColor 6060 with EXP6000 	DocuColor Windows NT based products with EFI front-ends are not affected by this vulnerability.

Product	Response to CERT[®] Advisory CA-2002-18
DocuColor Windows XPe based products with EFI front-ends: <ul style="list-style-type: none"> • DocuColor 3535 with EX3535 	The DocuColor Windows XPe based products with EFI front-ends are not affected by this vulnerability.
DocuColor with CREO front-ends: <ul style="list-style-type: none"> • DocuColor 2060/2045 with CSX2000 • DocuColor 3535 with CXP3535 • DocuColor 6060/2060 with CXP6000 	DocuColor products with CREO front-ends do not use SSH and are not, therefore, affected by this vulnerability.
DocuColor with EFI Splash front-ends: <ul style="list-style-type: none"> • DocuColor 12 with G640 • DocuColor 3535 with G3535 	DocuColor products with EFI Splash front-ends use Mac OS version 10.2.6 or later and are not, therefore, affected by this vulnerability.
Document Centre products (200, 300, 400 and 500 Series)	Document Centre products do not use OpenSSH and are not, therefore, affected by this vulnerability.
DocuPrint N Series products	DocuPrint N Series products do not use OpenSSH and are not, therefore, affected by this vulnerability.
DocuPrint NPS/IPS Series products	DocuPrint NPS/IPS Series products do not use OpenSSH and are not, therefore, affected by this vulnerability.
DocuSP-based products	DocuSP-based products do not use OpenSSH and are not, therefore, affected by this vulnerability.
Phaser products	Phaser products do not use OpenSSH and are not, therefore, affected by this vulnerability.
WorkCentre M35 WorkCentre M45 WorkCentre M55 WorkCentre Pro 35 WorkCentre Pro 45 WorkCentre Pro 55 WorkCentre Pro 65 WorkCentre Pro 75 WorkCentre Pro 90 WorkCentre Pro 32 Color WorkCentre Pro 40 Color	These WorkCentre products do not use OpenSSH and are not, therefore, affected by this vulnerability.

Contact

For additional information or clarification on any of the product information given here, contact Xerox support.

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.