

Xerox Product Response to CERT Advisory CA-2002-17: Apache Web Server Chunk Handling Vulnerability

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-2002-17](#) and [CERT Vulnerability Note VU#944335](#), issued by CERT on June 17, 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-2002-17](#) refers to the Apache web server (versions 1.2.2 and above, 1.3 through 1.3.24, and 2.0 through 2.0.36) and a remotely exploitable vulnerability in the way the server (or other web servers based on their source code) handle data encoded in chunks. Apache has released two new versions of the Apache web server (1.3.26 and 2.0.39) that correct this vulnerability.

Xerox Product Response

The table below lists various products and their positions with respect to [CERT Advisory CA-2002-17](#).

Product	Response to CERT Advisory CA-2002-17
DigiPath	DigiPath does not use the Apache web server and is not, therefore, affected by the vulnerability reported in CERT Advisory CA-2002-17 .
Document Centre products (DC220/230, DC332/340, DC432/440, DC255/265, DC460/470, DC460/470/480/490)	Document Centre products do not use the Apache web server and are not, therefore, affected by the vulnerability reported in CERT Advisory CA-2002-17 .
DocuPrint IPS, NPS	DocuPrint is not vulnerable because it uses Apache 1.3.19 in 32-bit mode only (and only in the DocuPrint 8 series, not in the DocuPrint 7 series). (The Apache advisory states "in Apache 1.3, the issue causes a stack overflow. Due to the nature of the overflow on 32-bit Unix platforms, this will cause a segmentation violation and the child will terminate.")
DocuShare	DocuShare is affected by the vulnerability reported in CERT Advisory CA-2002-17 . An hpptd update is available from http://docushare.xerox.com/View/Collection-7175 .
DocuSP-based products	DocuSP 3.6 pre-launch versions were impacted by this vulnerability. The vulnerability was corrected in the DocuSP 3.60.00 launch release.
DPServer	DPServer does not use the Apache web server and is not, therefore, affected by the vulnerability reported in CERT Advisory CA-2002-17 .

Product	Response to CERT Advisory CA-2002-17
EX12	EX12 is affected by the vulnerability reported in CERT Advisory CA-2002-17 . Xerox is working with Electronics for Imaging, Inc. (EFI) to ensure that patches are available soon.
EX2000 family	The EX2000 family of products is affected by the vulnerability reported in CERT Advisory CA-2002-17 . Xerox is working with Electronics for Imaging, Inc. (EFI) to ensure that patches are available soon.
EOMS	EOMS does not use the Apache web server and is not, therefore, affected by the vulnerability reported in CERT Advisory CA-2002-17 .
Flowport	Flowport does not use the Apache web server and is not, therefore, affected by the vulnerability reported in CERT Advisory CA-2002-17 .
Phaser products	Phaser products do not use the Apache web server and are not, therefore, affected by the vulnerability reported in CERT Advisory CA-2002-17 .
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 Pro products do not use the Apache web server and are not, therefore, affected by the vulnerability reported in CERT Advisory CA-2002-17 .

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.