

Xerox Product Response to US-CERT® Technical Cyber Security Alert TA04-099A: Cross-Domain Vulnerability in Outlook Express MHTML Protocol Handler

Audience and Purpose

The primary audience for this document is Xerox analysts and customers who want information regarding how Xerox products respond to [US-CERT® Technical Cyber Security Alert TA04-099A](#), issued by US-CERT® on April 8th, 2004. The following sections provide excerpts from the US-CERT® Technical Cyber Security Alert and the corresponding Xerox response.

Background

The [United States-Computer Emergency Readiness Team](#) (US-CERT) is a partnership between the National Cyber Security Division (NCSD) at the [Department of Homeland Security](#) (DHS) and the private sector. US-CERT provides individuals and organizations with access to valuable educational resources as well as up-to-date computer security information via the [National Cyber Alert System](#).

[US-CERT® Technical Cyber Security Alert TA04-099A](#) describes a cross-domain vulnerability in the Outlook Express MIME Encapsulation of Aggregate HTML Documents (MHTML) protocol handler that could allow an attacker to execute arbitrary code with the privileges of the user invoking the handler. The attacker may also be able to read and manipulate data on web sites in other domains or zones.

Xerox Product Response

The table below lists various products and their positions with respect to these vulnerabilities. The table will be updated with product information as it becomes available.

Product	Response to US-CERT® Technical Cyber Security Alert TA04-099A
CentreWare Network Scanning Services	CentreWare Network Scanning Services is not directly affected by this vulnerability. Operating systems on which CentreWare Network Scanning Services reside may be affected. We recommend that our customers install the latest operating system security patches.
CentreWare Network Services	CentreWare Network Services is not directly affected by this vulnerability. Operating systems on which CentreWare Network Services reside may be affected. We recommend that our customers install the latest operating system security patches.
DigiPath	The standard DigiPath configuration does not include Microsoft Outlook Express and is not, therefore, affected by this vulnerability.
DocuColor 1632/2240	The DocuColor 1632/2240 is not Windows-based and is not, therefore, affected by this vulnerability.
DocuColor 3535 with EFI Network Controller	DocuColor 3535 with EFI Network Controller is not Windows-based and is not, therefore, affected by this vulnerability.

Product	Response to US-CERT® Technical Cyber Security Alert TA04-099A
<p>DocuColor Windows 2000 based products with Creo front-ends:</p> <ul style="list-style-type: none"> • DocuColor 3535 with CXP3535 • DocuColor 6060/5252/2060/2045 with CXP6000 • DocuColor 5252/2045 with CXP5000 	<p>DocuColor Windows 2000 based products with Creo front-ends are affected by this vulnerability. Please use the following instructions to update your system, or contact your Xerox representative.</p> <p><u>Patch installation instructions:</u></p> <ol style="list-style-type: none"> 1. Exit the Spire application. 2. Download the Microsoft Hot Fix to the Spire Desktop. The Hot Fix can be found at http://www.microsoft.com/technet/security/bulletin/ms04-013.mspx 3. Install the appropriate Hot Fix. 4. If installation ended with a Restart/reboot prompt, press OK. 5. This completes the installation of the Hot Fix.
<p>DocuColor Windows NT based products with Creo front-ends:</p> <ul style="list-style-type: none"> • DocuColor 2060/2045 with CSX2000 	<p>DocuColor Windows NT based products with Creo front-ends are affected by this vulnerability. Please use the following instructions to update your system, or contact your Xerox representative.</p> <p><u>Patch installation instructions:</u></p> <ol style="list-style-type: none"> 1. Exit the Spire application. 2. Download the Microsoft Hot Fix to the Spire Desktop. The Hot Fix can be found at http://www.microsoft.com/technet/security/bulletin/ms04-013.mspx 3. Install the appropriate Hot Fix. 4. If installation ended with a Restart/reboot prompt, press OK. 5. This completes the installation of the Hot Fix.
<p>DocuColor Windows XP Professional SP1 based products with Creo front-ends:</p> <ul style="list-style-type: none"> • DocuColor 3535 with CXP3535e 	<p>DocuColor Windows XP Professional SP1 based products with Creo front-ends are affected by this vulnerability. Please use the following instructions to update your system, or contact your Xerox representative.</p> <p><u>Patch installation instructions:</u></p> <ol style="list-style-type: none"> 1. Exit the Spire application. 2. Download the Microsoft Hot Fix to the Spire Desktop. The Hot Fix can be found at http://www.microsoft.com/technet/security/bulletin/ms04-013.mspx 3. Install the appropriate Hot Fix. 4. If installation ended with a Restart/reboot prompt, press OK. 5. This completes the installation of the Hot Fix.
<p>DocuColor Windows XP Professional SP2 based products with Creo front-ends:</p> <ul style="list-style-type: none"> ▪ DocuColor 3535 with CXP3535e 	<p>DocuColor Windows XP Professional SP2 based products with Creo front-ends include the fix and are not, therefore, affected by this vulnerability.</p>
<p>DocuColor with EFI Splash front-ends:</p> <ul style="list-style-type: none"> • DocuColor 12 with G640 • DocuColor 3535 with G3535 	<p>DocuColor products with EFI Splash front-ends are not Windows-based and are not, therefore, affected by this vulnerability.</p>
<p>Document Centre products (200, 300, 400 and 500 Series)</p>	<p>Document Centre products are not Windows-based and are not, therefore, affected by this vulnerability.</p>

Product	Response to US-CERT® Technical Cyber Security Alert TA04-099A
DocuPrint N Series products	DocuPrint N Series products are not Windows-based and are not, therefore, affected by this vulnerability.
DocuPrint NPS/IPS Series products	DocuPrint NPS/IPS Series products are not Windows-based and are not, therefore, affected by this vulnerability.
DocuSP-based products	DocuSP-based products are not Windows-based and are not, therefore, affected by this vulnerability.
FaxCentre F12	The FaxCentre F12 is not Windows-based and is not, therefore, affected by this vulnerability.
Flowport	Flowport is not directly affected by this vulnerability. Operating systems on which Flowport resides may be affected. We recommend that our customers install the latest operating system security patches.
FreeFlow SMARTsend	FreeFlow SMARTsend is not directly affected by this vulnerability. Operating systems on which SMARTsend resides may be affected. We recommend that our customers install the latest operating system security patches.
Phaser products	Phaser products are not Windows-based and are not, therefore, affected by this vulnerability.
WorkCentre M15 WorkCentre M24 WorkCentre M35 WorkCentre M45 WorkCentre M55 WorkCentre PE16 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 WorkCentre Pro 423 WorkCentre Pro 428	These WorkCentre products are not Windows-based and are not, therefore, affected by this vulnerability.

Product	Response to US-CERT® Technical Cyber Security Alert TA04-099A
<p>Xerox products with EFI Windows NT based front ends with Fiery Advanced Controller Interface (FACI):</p> <ul style="list-style-type: none"> • DocuColor 12 with X12 • DocuColor 12 with EX12 • DocuColor 12 with XP12 • DocuColor 40 with X40 • DocuColor 2045/2060 with EX2000 • DocuColor 2045/2060/5252 with EX2000d • DocuColor 2045/2060 with EX2000v • Xerox 1010 with EX1010 	<p>Xerox products with EFI Windows NT based front ends with FACI do not include Microsoft Outlook Express and are not, therefore, affected by this vulnerability.</p>
<p>Xerox products with EFI Windows NT based front ends <u>without</u> Fiery Advanced Controller Interface (FACI):</p> <ul style="list-style-type: none"> • DocuColor 12 with X12 • DocuColor 12 with EX12 • DocuColor 12 with XP12 • DocuColor 40 with X40 • Xerox 1010 with EX1010 	<p>Xerox products with EFI Windows NT based front ends without FACI do not include Microsoft Outlook Express and are not, therefore, affected by this vulnerability.</p>
<p>Xerox products with EFI Windows XPe based front ends with Fiery Advanced Controller Interface (FACI):</p> <ul style="list-style-type: none"> • DocuColor 12 with X12/EX12/XP12 (customer purchased s/w option) • DocuColor 3535 with EX3535 • DocuColor 5252 with EXP5000 • DocuColor 6060 with EXP6000 • DocuColor 8000 with EXP8000 • Phaser EX7750 • Xerox 2101 with EX2101 	<p>Xerox products with EFI Windows XPe based front ends with FACI do not include Microsoft Outlook Express and are not, therefore, affected by this vulnerability.</p>

Product	Response to US-CERT® Technical Cyber Security Alert TA04-099A
<p>Xerox products with EFI Windows XPe based front ends <u>without</u> Fiery Advanced Controller Interface (FACI):</p> <ul style="list-style-type: none">• DocuColor 12 with X12/EX12/XP12 (customer purchased s/w option)• DocuColor 3535 with EX3535• Phaser EX7750• Xerox 2101 with EX2101	<p>Xerox products with EFI Windows XPe based front ends without FACI do not include Microsoft Outlook Express and are not, therefore, affected by this vulnerability.</p>

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.