

Xerox Product Response to CERT[®] Vulnerability Note VU#838572: *Microsoft Authenticode mechanism installs ActiveX controls without prompting user (MS03-041)*

The primary audience for this document is Xerox analysts and customers who want information regarding how Xerox products respond to [CERT[®] Vulnerability Note VU# 838572](#), issued by CERT[®] on October 16th, 2003. 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[®] Vulnerability Note VU# 838572](#) describes a vulnerability in Microsoft's Authenticode that could allow a remote attacker to install an untrusted ActiveX control on the victim's system.

Xerox Product Response

The table below lists various products and their positions with respect to [CERT[®] Vulnerability Note VU# 838572](#). This document will be updated with additional product information as it becomes available.

| Product | Response to CERT[®] Vulnerability VU# 838572 |
|---|--|
| CentreWare Network Scanning Services | CentreWare Network Scanning Services is not affected by this vulnerability. |
| CentreWare Network Services | CentreWare Network Services is not affected by this vulnerability. |

| Product | Response to CERT® Vulnerability VU# 838572 |
|-----------------------------------|---|
| <p>DigiPath</p> | <p>DigiPath products are affected by this vulnerability.</p> <p><u>Instructions for using Windows Update on DigiPath version 3.0/4.0</u></p> <ol style="list-style-type: none"> 1. Ensure that a TapeWare system backup exists. 2. On a weekly basis, run Windows Update: <ol style="list-style-type: none"> a. Open up Windows Internet Explorer. b. From the Tools menu, select "Windows Update". c. If prompted to install the latest Windows Update software, select [Yes]. Then select [Yes] to reboot your machine. If you did not receive this prompt, proceed to step f. d. Open up Windows Internet Explorer. e. From the tools menu, select "Windows Update". f. Select "Scan for Updates" in the main center window. g. In the left window pane, select "Critical Updates and Service Packs". h. Select "Review and Install Updates". i. Select [Install Now] to download all the Microsoft critical updates needed for your system. j. Select [Accept] to accept the Microsoft license agreement. k. The patches will be downloaded and installed. l. If prompted, select [Yes] to restart your system. <p>Note: Service Packs are not to be installed via this process. When prompted by the Service Pack install message, select "Cancel" to return to the "Install Now" screen, and remove the service pack from the list of downloads. Continue with the rest of the patches by selecting "Install Now".</p> <p><u>Instructions for using Windows Update on DigiPath version 2.1 (Windows NT)</u></p> <p>Note: DigiPath 1.2 customers can follow these DigiPath 2.1 instructions at their own risk.</p> <ol style="list-style-type: none"> 1. Ensure that a TapeWare system backup exists. 2. On a weekly basis, run Windows Update: <ol style="list-style-type: none"> a. Go to URL: http://windowsupdate.microsoft.com b. The product catalog will be updated for your system. c. Windows Update will customize the product update catalog for your system. d. Only critical updates will be automatically selected. e. Select the Download button in the top right window pane. f. Select [Start Download]. g. Select [Yes] to accept the license agreement. h. The patches will be downloaded and installed. <p>If prompted, select [Yes] to restart your system.</p> |
| <p>DocuColor 1632/2240</p> | <p>The DocuColor 1632/2240 products do not include the Windows Operating System and are not, therefore, affected by this vulnerability.</p> |

| Product | Response to CERT® Vulnerability VU# 838572 |
|--|--|
| DocuColor 2060/2045 with CSX2000 | <p>DocuColor 2060/2045 with CSX2000 is 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/downloads/details.aspx?FamilyId=21F64FF0-9175-42BE-A8E4-BDC59A98BDF2&displaylang=en 3. Double-click the Hot Fix to run. 4. If installation ended with a Restart/reboot prompt, press OK. 5. This completes the installation of the Hot Fix. |
| DocuColor Windows XPe based products with EFI front-ends: <ul style="list-style-type: none"> • DocuColor 3535 with EX3535 | <p>DocuColor Windows XPe based products with EFI front-ends are affected by this vulnerability. Patch 1-DSRD9 can be downloaded from the 'Critical Security Updates' section of the DocuColor 3535's Drivers and Downloads page.</p> |
| DocuColor with Creo front-ends: <ul style="list-style-type: none"> • DocuColor 3535 with CXP3535 • DocuColor 6060/2060 with CXP6000 | <p>DocuColor products with CREO front-ends are affected by this vulnerability. Please use the following instructions to update your system, or you may 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/downloads/details.aspx?FamilyId=90D27AEC-7D2A-45FD-B85A-E98E574338F1&displaylang=en 3. Double-click the Hot Fix to run. 4. If installation ended with a Restart/reboot prompt, press OK. 5. This completes the installation of the Hot Fix. |
| DocuColor 3535 with EFI Network Controller | <p>DocuColor 3535 with EFI Network Controller is Linux-based and is not, therefore, affected by this vulnerability.</p> |
| DocuColor with EFI Splash front-ends: <ul style="list-style-type: none"> • DocuColor 12 with G640 • DocuColor 3535 with G3535 | <p>DocuColor products with EFI Splash front-ends are Macintosh based and are not, therefore, affected by this vulnerability.</p> |
| Document Centre products (200, 300, 400 and 500 Series) | <p>Document Centre products are not built on Microsoft Windows and are not, therefore, affected by this vulnerability.</p> |

| Product | Response to CERT® Vulnerability VU# 838572 |
|---|---|
| Document Centre Xerox WIA Driver for Microsoft® Windows XP® | Document Centre Xerox WIA Driver for Microsoft® Windows XP® is not affected by this vulnerability. |
| DocuPrint N Series products | DocuPrint N Series products do not include the Windows Operating System and are not, therefore, affected by this vulnerability. |
| DocuPrint NPS/IPS Series products | DocuPrint NPS/IPS Series products are Sun based and are not, therefore, affected by this vulnerability. |
| DocuSP-based products | DocuSP based products are Sun Solaris based and are not, therefore, affected by this vulnerability. |
| FlowPort | FlowPort is not affected by this vulnerability. |
| iGen3 Creo Spire Color Controller | <p>The iGen3 Creo Spire Color Controller is affected by this vulnerability. Please use the following instructions to update your system, or you may 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/downloads/details.aspx?FamilyId=90D27AEC-7D2A-45FD-B85A-E98E574338F1&displaylang=en 3. Double-click the Hot Fix to run. 4. If installation ended with a Restart/reboot prompt, press OK. 5. This completes the installation of the Hot Fix. |
| Phaser products | Phaser products do not include the Windows Operating System and are not, therefore, affected by this vulnerability |
| WorkCentre M24 | The WorkCentre M24 does not include the Windows Operating System and is 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 are not built on Microsoft Windows and are not, therefore, affected by this vulnerability. |

| Product | Response to CERT® Vulnerability VU# 838572 |
|-------------------|--|
| Xerox 2101 | The Xerox 2101 is affected by this vulnerability. Patch 1-DSRD9 can be downloaded from the 'Critical Security Updates' section of the Xerox 2101's Drivers and Downloads page. |

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.