

BOLETIM DE SEGURANÇA XEROX XRX05-007

Vulnerabilidades no Xerox MicroServer Web Server podem potencialmente permitir o acesso não autorizado.

A seguinte solução de software e instruções de auto-serviço, destinam-se aos produtos listados de modo a proteger os seus dados confidenciais de possíveis violações através da rede.

A solução de software está comprimida num ficheiro zip de 1,7 MB a que pode aceder usando o seguinte link em Xerox.com / Security:

http://www.xerox.com/downloads/usa/en/c/cert_P23_HTTP_Patch_AllWCP.zip

Histórico

Existem algumas vulnerabilidades no código do servidor web que poderão permitir o acesso não autorizado ao servidor web e que incluem:

- Vulnerabilidades que podem ignorar a autenticação.
- Pedidos HTTP especialmente construídos que podem rejeitar o serviço ou permitir o acesso não autorizado a ficheiros num equipamento atacado.
- Scripting entre vários sites permitindo alterar conteúdo de páginas web de um modo não autorizado.

Caso seja bem sucedido, um intruso pode efectuar alterações não autorizadas à configuração do sistema. As passwords de cliente e utilizador não estão expostas.

Esta solução de software é cumulativa e integra as soluções de software documentadas nos Boletins de Segurança XRX04-002 (P4), XRX04-007 (P10), XRX04-009 (P17) e XRX05-005 (P21) para os produtos indicados em baixo.

Produtos Afectados:

WorkCentre®	WorkCentre® Pro
M35	32 Color
M45	35
M55	40 Color
M165	45
M175	55
	65
	75
	90
	165
	175

Solução

Processo de Instalação do Patch WebUI Edição: 15 de Julho de 2005

Existe um software de solução (patch) que resolve as vulnerabilidades do Xerox MicroServer Web Server que foram identificadas em Equipamentos Multi-funcionais (MFD) WorkCentre. O software de solução (patch) apenas precisa ser aplicado ao MFD se a versão de software de Sistema se encontrar na lista abaixo. Este software de solução substitui as anteriores soluções P3, P4, P10, P17, P20 e P21.

Precisa descarregar o patch. O patch encontra-se em formato ZIP. Descarregue o ficheiro ZIP do URL indicado e retire todo o conteúdo para o seu PC. **NÃO TENHA ABRIR O FICHEIRO COM A EXTENSÃO .TGZ** Este é o software de solução e deve ser carregado no MFD tal como está.

Instruções de Instalação

Nome do ficheiro: **P23_http_AIIWCP.tgz**

Este software de solução apenas será preciso se o Software de Sistema do seu WorkCentre se incluir nas seguintes versões:

WorkCentre M35/M45/M55 versão 2.028.11.000 até 2.97.20.048

ou versão 4.84.16.000 até 4.97.20.048

WorkCentre Pro 35/45/55 versão 3.028.11.000 até 3.97.20.048

WorkCentre Pro 65/75/90 versão 1.001.00.060 até 1.001.02.706

WorkCentre Pro 32/40 Color versão 0.001.00.060 até 0.001.02.707

WorkCentre M165/M175 versão 6.47.30.000 até 6.57.32.007

ou versão 8.47.30.000 até 8.57.32.007

WorkCentre Pro 165/175 versão 7.47.30.000 até 7.57.32.007

Se o seu equipamento tiver um Software de Sistema com uma versão superior não precisa instalar o software de solução.

Confirme a Versão de Software do Sistema

Para saber qual a versão do seu Software de Sistema, pode imprimir um Relatório de Configuração ou ver a versão na interface de cliente na Web.

Para imprimir um relatório de configuração a partir da Interface de Utilizador no equipamento:

- 1) Prima o botão Estado do Equipamento
- 2) Seleccione Imprimir Relatório de Configuração
- 3) Procure o número da Versão de Software do Sistema.

Para ver o número da versão a partir da interface de cliente na web:

- 1) Abra um web browser e ligue-se ao equipamento multifuncional digitando o endereço IP do equipamento.
- 2) Seleccione o ícone "Index" na metade superior do ecrã
- 3) Seleccione "Configuração".
- 4) Vá até ao local de "Printer Setup" que mostra a Versão de Software do Sistema.

Instalar o Software

NÃO TENHA ABRIR O FICHEIRO DO SOFTWARE POIS PODERÁ DANIFICÁ-LO.

Neste modelo, o software pode ser enviado de dois modos.

- 1) Método LPR
- 2) Método de Upgrade do Software do Equipamento

Método LPR a partir de Windows NT, 2000 ou XP

Este método exige que tenha activado um Protocolo LPR no equipamento. Verifique o relatório de configuração para confirmar se o protocolo está activado. Este protocolo pode ser activado através do Interface de Utilizador Local ou do Interface Web. Veja mais instruções no Apêndice A.

- 1) Abra uma janela "DOS Command Prompt". Pode fazer isto seleccionando o ícone "Start" do Windows e depois seleccionando "Run". Digite "cmd" e prima <Enter>.
- 2) Submeta o ficheiro de software através da linha de comando: **lpr -S <printer_ip> -Pip **P23_http_AIIWCP.tgz****
- 3) O WorkCentre reinicia-se automaticamente para instalar o software.
- 4) O software estará instalado quando **.P23** estiver adicionado ao número da versão do Controlador de Rede.

Método de Upgrade do Software do Equipamento

- 1) Abra um web browser e ligue-se ao equipamento multifuncional digitando o endereço IP do equipamento.
- 2) Selecciono o ícone "Index" na metade superior do ecrã.
- 3) Selecciono "Software do Equipamento (Upgrades)".
- 4) Digite o Nome de Utilizador, Admin e Password de Admin do equipamento.
- 5) Em "Upgrade Manual" seleccione o botão Procurar para procurar e seleccionar o ficheiro **P23_http_AIIWCP.tgz**
- 6) Selecciono o botão "Instalar Software".
- 7) O WorkCentre reinicia-se automaticamente para instalar o software.
- 8) O software estará instalado quando **.P23** estiver adicionado ao número da versão do Controlador de Rede. O WorkCentre M35/M45/M55 e M165/M175 NÃO mostra **.P23**, mas o software está instalado.

Limites de Responsabilidade

A informação fornecida neste Xerox Product Response é fornecida "tal como está" sem quaisquer garantias. A Xerox Corporation renuncia quaisquer garantias, expressas ou implícitas, incluindo as garantias de comerciabilidade e de que o equipamento seja adequado a um determinado fim. Em caso algum será a Xerox Corporation responsável por quaisquer danos que resultem da má utilização ou não respeito pela informação fornecida neste Xerox Product Response, incluindo perda de negócio directa, indirecta, acidental ou consequencial, ou danos especiais, mesmo tendo a Xerox Corporation sido avisada da possibilidade desses danos. Alguns países não permitem a exclusão ou limites de responsabilidade por danos consequenciais, não se aplicando deste modo os limites acima descritos.