

BOLETIM DE SEGURANÇA XEROX XRX06-004

Actualização acumulada direccionada a várias vulnerabilidades de segurança.

Versões de Software de Sistema 12.050.03.000, 14.050.03.000 ou 13.050.03.000, dependendo se o produto é um WorkCentre[®] ou WorkCentre[®] Pro, é uma actualização a Versões do Software de Sistema 12.027.24.000, 14.027.24.000 e 13.027.24.000, respectivamente, que inclui soluções de segurança para o software de sistema. Consulte o Apêndice A das Instruções de Instalação para obter o Software de Sistema *.50.03.000.¹.

Aconselhamos os clientes a actualizarem os seus equipamentos com o Software de Sistema Versão 12.050.03.000, 14.050.03.000 ou 13.050.03.000, respectivamente. A tabela abaixo, mostra a versão correspondente do Controlador de Rede para cada uma destas três Versões de Software de Sistema.

Versão do SW de Sistema	Versão do Controlador de Rede
12.050.03.000.	040.010.01172
13.050.03.000.	040.010.51172
14.050.03.000.	040.010.11172

Histórico

Software de Sistema das Versões 12.050.03.000, 14.050.03.000 e 13.050.03.000 são releases de manutenção que incluem soluções de segurança para Software de Sistema das Versões 12.027.24.000, 14.027.24.000 e 13.027.24.000, respectivamente. A actualização inclui soluções de segurança para as seguintes vulnerabilidades no ESS/ Controlador de Rede e MicroServer Web Server code:

- A autenticação na Interface Web do Utilizador pode ser ultrapassada.
- US-CERT Technical Cyber Security Alert TA04-174A.
- A versão Samba deve ser actualizada para responder a várias vulnerabilidades.
- SNMP Agent não devolve um erro de objectos só de leitura.
- SNMP Authentication failure traps não podem ser activadas ou geradas.
- Vulnerabilidade no Controlador de Rede: http TRACE XSS attack.
- PS script anexado provoca o crash de ops3-dmn com core dump; DoS attack.
- Partilha SMB "Homes" visível.
- Possibilidade de pesquisar ficheiro de sistema SMB.
- Possibilidade de download anónimo de Audit Log.
- Problemas de Segurança HTTP.
- Ultrapassa segurança e arranca o Alchemy usando USB "thumb drive" (ou outro método).
- Pesquisar "Validate Repository SSL Certificate" não verificando FQDN.
- Determinadas autorizações a ficheiro devem ser mais rigorosas.
- Segurança Linux - Necessário solucionar vulnerabilidade kernel CAN-2003-0643 - problema no socket.
- Porta 443 está sempre activa - má configuração httpd.conf.
- Bloqueio de porta Postgress.
- SNMP Authentication failure traps não podem ser activadas nem geradas.
- Fragmentos CRÍTICOS de dados remanescentes do utilizador em http.log após Sobreposição Imediata de Imagem (IIO).

¹* será 12, 13, ou 14 dependendo do produto ser um WorkCentre[®] ou um WorkCentre[®] Pro

- Mensagem de Erro IIO em LUI se sobreposição falhar.
- Quando Trabalho Retido é apagado, IIO reporta uma falha.
- Sobreposição de Imagem a Pedido falha se sobreposição for superior a 2GB.

Se estas vulnerabilidades forem exploradas com sucesso, as funções de segurança podem não funcionar devidamente e um intruso poderá conseguir acesso não autorizado e fazer alterações não autorizadas na configuração do sistema. As passwords de cliente e utilizador não estão expostas.

Produtos Afectados:

WorkCentre®	WorkCentre® Pro
232	232
238	238
245	245
255	255
265	265
275	275

Apêndice A

Obter Software de Sistema Versão *.50.03.000

Para obter a release geral mais recente:

- a) Use um browser para entrar em www.xerox.pt.
- b) Seleccione o link "Suporte e Drivers".
- c) Seleccione "Multifuncionais".
- d) Seleccione "WorkCentre" ou "WorkCentre Pro" de acordo com o seu modelo
- e) Procure o link para o seu modelo de WorkCentre.
- f) Seleccione "Drivers e Downloads".
- g) Seleccione o link para "Firmware & Machine Upgrades".
- h) Seleccione o link para "System software version *.50.03.000 install instructions" e imprima ou grave estas instruções.
- i) Seleccione o link para "System Software Upgrade Version *.50.03.000" e grave o ficheiro no seu computador.
- j) Após ter feito o download, extraia os ficheiros para a sua desktop.
- k) Reveja o documento dc06cc0406.pdf que está incluído, para obter informação adicional sobre o upgrade do seu equipamento.
- l) Reveja o documento "System Software Install Instructions" que gravou.
- m) Faça upgrade do equipamento.
- n) Volte a secção "Install the Patch".

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, accidental 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.