

XEROX BOLETIM DE SEGURANÇA XRX06-006

Atualização acumulativa para endereçar vulnerabilidades múltiplas de segurança.

Versões do Software do Sistema 12.060.17.000, 14.060.17.000 ou 13.060.17.000, dependendo do produto, se for um WorkCentre[®] ou WorkCentre[®] Pro, são uma atualização das Versões do Software do Sistema 12.050.03.000, 14.050.03.000 e 13.050.03.000, respectivamente, que inclui correções de segurança para o software do sistema. Consulte o Anexo A para obter o software do sistema *.060.17.000¹.

Recomenda-se fortemente aos clientes que atualizem seus dispositivos para a Versão do Software do Sistema 12.060.17.000, 14.060.17.000 ou 13.060.17.000, respectivamente. Siga os procedimentos no Anexo A para obter o software do sistema atualizado. Utilize as instruções de instalação do cliente que acompanham o software do sistema para atualizar seu dispositivo. A tabela abaixo mostra a versão da Controladora de rede correspondente para cada uma destas três Versões de Software do Sistema.

Produtos	Versão de SW do Sistema	Versão da Controladora de rede
WorkCentre 232/238/245/255/265/275	12.060.17.000.	040.022.00115
WorkCentre Pro 232/238/245/255/265/275	13.060.17.000.	040.022.50115
WorkCentre 232/238/245/255/265/275 com opção PostScript	14.060.17.000.	040.022.10115

Informações importantes

Versões do Software do Sistema 12.060.17.000, 14.060.17.000 e 13.060.17.000 são versões de manutenção que incorporam correções de segurança para as Versões do Software do Sistema 12.050.03.000, 14.050.03.000 e 13.050.03.000, respectivamente. A atualização incorpora correções de segurança para as seguintes vulnerabilidades no código de ESS/Controladora de Rede e do Servidor de Web MicroServer:

- nome do host TCP/IP na Interface com o usuário da Web vulnerável à injeção de comandos.
- Campo do nome da pasta Scan-to-mailbox (Digitalizar para caixa postal) na Interface com o usuário da Web vulnerável à injeção de comandos.
- Parâmetros de configuração da rede Microsoft na Interface com o usuário da Web vulnerável à injeção de comandos.
- Permissões de Navegador podem permitir acesso não autorizado.
- A opção de configuração automática de TFTP/BOOTP pode permitir a configuração não autorizada das definições.
- As solicitações de serviços da Web podem ser feitas com o uso de HTTP ao invés de HTTPS.
- A assinatura de mensagens de e-mail pode ser capturada para exibir itens impróprios.
- A função Scan-to-mailbox (Digitalizar para caixa postal) pode permitir o download anônimo e não autenticado de arquivos seguros.
- O dispositivo não manteve a hora exata, portanto as marcações de hora nos registros de auditoria ficaram incorretas.

Se estas vulnerabilidades forem exploradas com sucesso, as funções de segurança podem não funcionar corretamente e uma pessoa não credenciada poderá cometer um ataque para obter acesso não autorizado e fazer alterações não autorizadas à configuração do sistema. As senhas de cliente e de usuário não estão expostas.

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

Além das correções acima, temos destacado a segurança dos arquivos de atualização de DLM, incorporando assinaturas digitais.

Produtos afetados:

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

Anexo A**Obtenção da Versão do Software do Sistema mais recente**

Para obter a versão mais recente:

- a) Use um navegador para acessar www.xerox.com.
- b) Selecione o link chamado "Suporte & Drivers".
- c) Selecione "Multifuncionais".
- d) Selecione "WorkCentre" ou "WorkCentre Pro", dependendo do seu modelo.
- e) Localize o link para o seu modelo de WorkCentre.
- f) Selecione "Drivers e Downloads".
- g) Selecione o link para "Firmware & Atualizações da máquina".
- h) Selecione o link para "Instruções de instalação do Software do Sistema versão xx.xx.xx.xxx" e imprima ou salve estas instruções.
- i) Selecione o link para "Atualização do Software do Sistema versão xx.xx.xx.xxx" e salve o arquivo no seu computador.
- j) Uma vez concluído o download, extraia os arquivos para a área de trabalho do seu computador.
- k) Reveja as "Instruções de Instalação do Software do Sistema" que você salvou quanto a informações importantes sobre a atualização do seu dispositivo.
- l) Atualize o dispositivo.
- m) Retorne à seção "Instalar o Patch" no documento mencionado acima.

Isenção de responsabilidade

As informações nesta Resposta sobre Produto Xerox são fornecidas "como estão" sem garantias de qualquer espécie. A Xerox Corporation se isenta de todas as garantias, expressas ou implícitas, inclusive as de comercialização e adequação para um fim específico. Em nenhuma circunstância a Xerox Corporation será responsável por quaisquer danos resultantes da utilização ou descaso do usuário quanto às informações fornecidas nesta Resposta sobre o Produto Xerox, inclusive sobre os danos diretos, indiretos, incidentais, consequenciais, perdas por lucros cessantes ou danos especiais, mesmo que a Xerox Corporation tenha sido avisada sobre a possibilidade desses danos. Alguns estados não permitem a exclusão ou limitação de responsabilidade por danos consequenciais, assim, a limitação descrita acima pode não se aplicar.