

SL Workstation atualização de segurança ("PrintNightmare")



Seeing beyond

SL Workstation atualização de segurança (“PrintNightmare”)

Observação: este documento não substitui o manual do usuário fornecido com o dispositivo.

Sobre a atualização

“PrintNightmare” é o nome de uma falha de segurança que atinge dispositivos que funcionam com sistemas operacionais (OS) Microsoft Windows. Segundo a Microsoft, “Há uma vulnerabilidade de execução de código remoto quando o serviço Windows Print Spooler executa operações de arquivo de forma indevida com determinadas permissões. Um invasor poderia explorar com sucesso esta vulnerabilidade e executar códigos arbitrários com permissões do sistema. O invasor poderia instalar programas, visualizar dados, modificar ou excluir ou criar novas contas com direitos de usuário ilimitados.”

O “PrintNightmare” não prejudica a segurança nem o funcionamento do ZEISS SL Workstation. Contudo, oferecemos uma atualização de segurança (Patch) para o ZEISS SL Workstation, a fim de solucionar a vulnerabilidade causada pelo “PrintNightmare”.

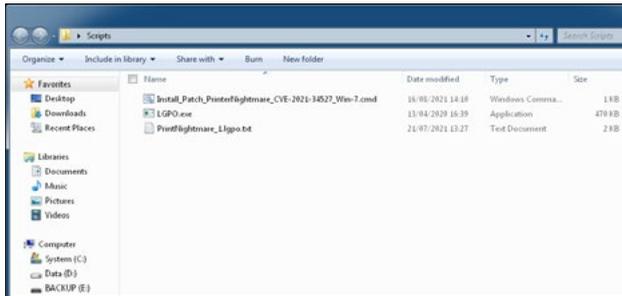
Mídia de armazenamento necessária

Para fazer o download da atualização antes da instalação, é necessário um dispositivo de memória USB vazio com pelo menos 1 GB de capacidade de armazenamento.

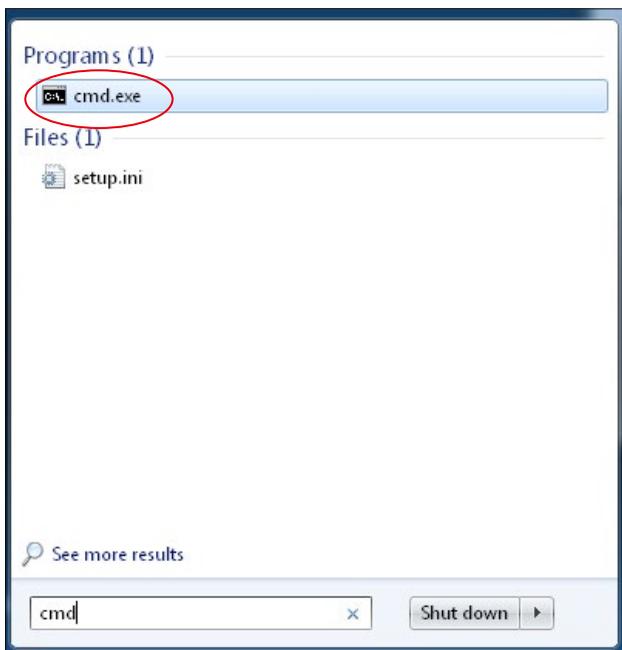
Preparação

- Faça o download dos arquivos a seguir e salve-os diretamente no diretório raiz do dispositivo USB:
 - LGPO.exe
 - PrintNightmare_1.lgpo.txt
 - Install_Patch_PrinterNightmare_CVE-2021-34527_Win-7.cmd

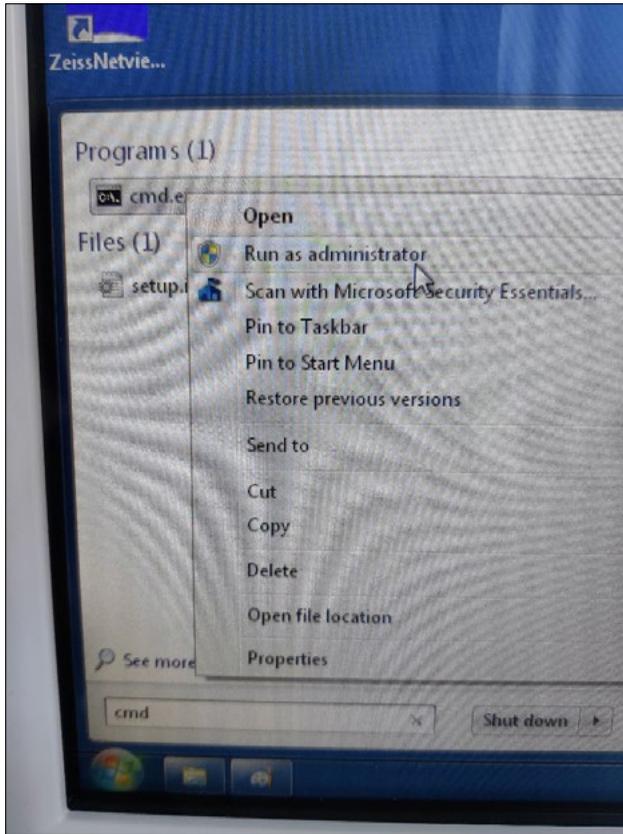
Como instalar a atualização para o ZEISS SL Workstation



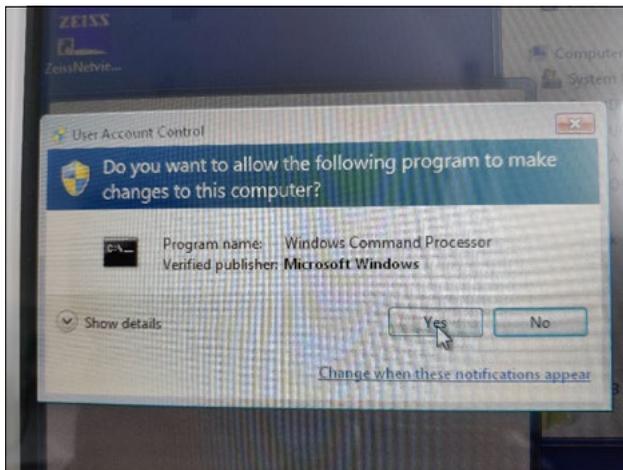
1. Ligue o SL Workstation.
2. Conecte o dispositivo USB com os arquivos de atualização.
3. Copie os três arquivos na seguinte ordem: C:\Users\Zeiss\Desktop\Scripts. Certifique-se de que o arquivo com a extensão .cmd contenha a abreviação "Win-7" no nome.



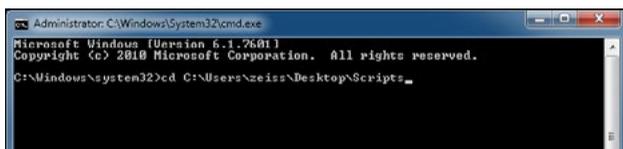
4. Abra o menu inicial do computador pelo botão do Windows e insira "cmd" na lista de pesquisa. Na tela, é exibida uma tarefa semelhante à ilustração ao lado.



5. Clique com o botão direito em “cmd.exe”, para abrir o menu de contexto. Selecione “Run as administrator” (Executar como administrador).



6. Uma nova janela é aberta na tela. Selecione “Yes” (Sim), para acionar um prompt de comando.



7. É aberta uma janela para o prompt de comando (administrador). Insira “cd c:\users\zeiss\Desktop\scripts” e pressione Enter.

```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Versão 6.1.7601]
Copyright (c) 2010 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Users\zeiss\Desktop\Scripts
C:\Users\zeiss\Desktop\Scripts>install_patch_printerNightmare_CVE-2021-34527_Win-7.cmd
```

8. Após a modificação do diretório, insira "Install" e pressione a tecla TAB. O nome do arquivo deve ser preenchido como mostrado na figura ao lado. Clique em Enter para continuar.

```
Administrator: C:\Windows\System32\cmd.exe - install_patch_printerNightmare_CVE-2021-34527_Win-7.cmd
C:\Users\zeiss\Desktop\Scripts>install_patch_printerNightmare_CVE-2021-34527_Win-7.cmd
OK : 1 LGPO compiled and registered.

SERVICE_NAME: lpdsvc
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE                : 3  STOP_PENDING
                        CANNOT_STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE       : 0  <0x0>
        SERVICE_EXIT_CODE   : 0  <0x0>
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x0

SERVICE_NAME: spooler
        TYPE               : 110  WIN32_OWN_PROCESS (interactive)
        STATE                : 3  STOP_PENDING
                        CANNOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE       : 0  <0x0>
        SERVICE_EXIT_CODE   : 0  <0x0>
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x420

This shared resource does not exist.

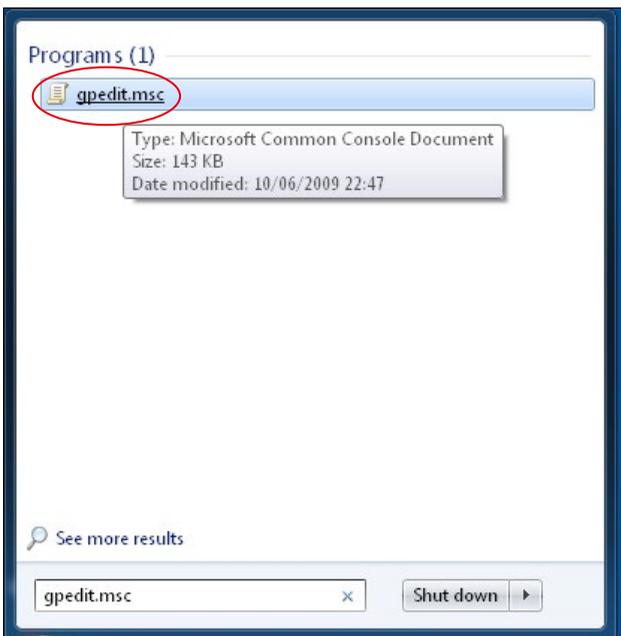
More help is available by typing NET HELPMSG 2310.

SERVICE_NAME: spooler
        TYPE               : 110  WIN32_OWN_PROCESS (interactive)
        STATE                : 2  START_PENDING
                        CANNOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE       : 0  <0x0>
        SERVICE_EXIT_CODE   : 0  <0x0>
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x7d0
        PID                 : 7500
        FLAGS                :

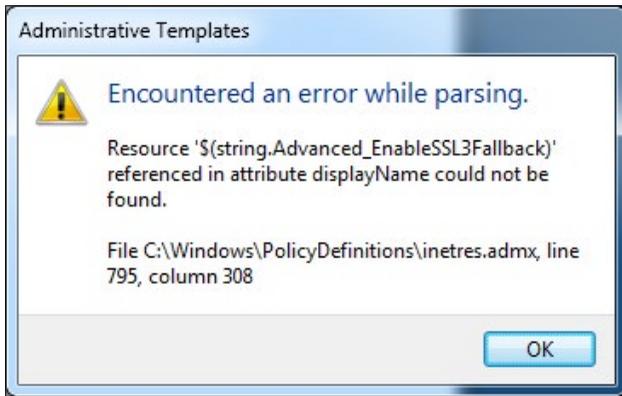
SERVICE_NAME: lpdsvc
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE                : 2  START_PENDING
                        CANNOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE       : 0  <0x0>
        SERVICE_EXIT_CODE   : 0  <0x0>
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x7d0
        PID                 : 1372
        FLAGS                :

OK : Print spooler service restarted.
Press any key to continue . . .
```

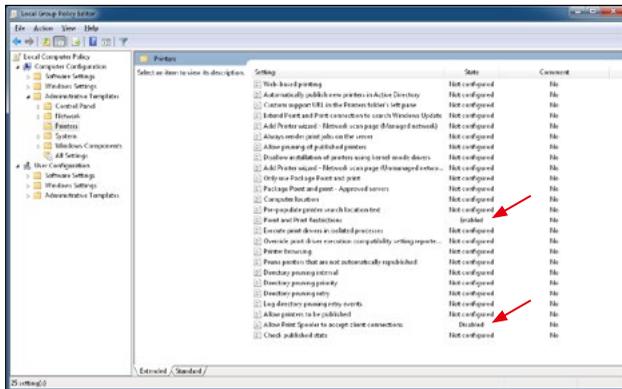
9. O script é executado.
10. Após a conclusão bem-sucedida da execução do script, reinicie o computador para que as modificações sejam incorporadas.



11. Após o reinício bem-sucedido do computador, abra o menu inicial do computador usando botão do Windows e insira "gpedit" na lista de pesquisa. Clique no item com a correspondência mais alta para abrir as configurações das Políticas de Grupo.



12. A mensagem de aviso ao lado aparecerá duas vezes. Confirme a mensagem com “OK”.



13. A janela para edição das Políticas de Grupo é aberta. Clique em “Computer Configuration” (Configuração do computador) > “Administrative Templates” (Modelos administrativos) > “Printers” (Impressora). Certifique-se de que “Point and Print Restrictions” (Restrições Point-and-Print) esteja ativo (“Enabled”) e a configuração “Allow Print Spooler to accept client connections” (Permitir que as conexões do cliente sejam aceitas no spooler de impressão) esteja desativada (“Disabled”).

Explore mais vídeos especializados, documentos de ajuda, perguntas e respostas no ZEISS Product Insights.



A página web de ZEISS Product Insights



Carl Zeiss Meditec AG

Göschwitzer Strasse 51-52

07745 Jena, Alemanha

www.zeiss.com/med

info.meditec@zeiss.com

000000-2279-200-AddGA-BR-260821