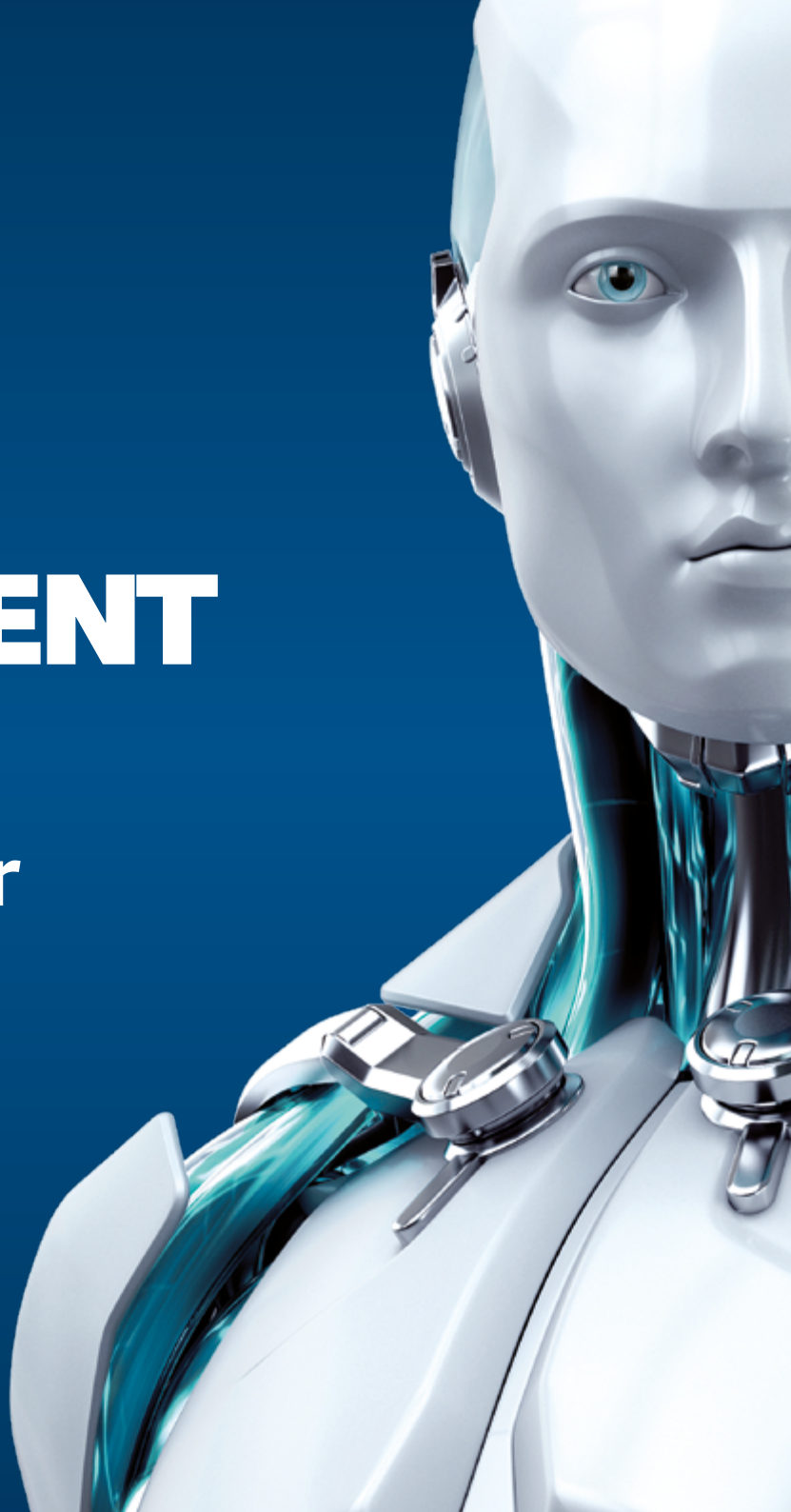
FLEXERA SOFTWARE

PATCH MANAGEMENT

Requisitos do sistema para Corporate Software Inspector



ESET TECHNOLOGY ALLIANCE

Flexera

Administração de patches com Corporate Software Inspector

Corporate Software Inspector gerencia quando, onde e como acontece a instalação de patches de segurança. Avisa quando há um patch disponível para uma vulnerabilidade de software que está ameaçando sua infraestrutura, onde terá maior impacto, que estratégia de solução é a mais adequada e como implementá-la.

Secunia Research verifica continuamente as vulnerabilidades e a eficácia dos patches publicados pelos vendedores. Estes dados logo se adaptam à sua infraestrutura específica, possibilitando priorizar, planificar e executar fluxos de trabalho, assim como documentar os esforços para reduzir riscos.

REQUISITOS

Requisitos do sistema para Corporate Software Inspector (CSI) 7.0

CSI 7.0 é uma solução baseada na Web completamente funcional para usar com a última versão do Internet Explorer. Os resultados dos rastreamentos também podem ser visualizados em outros navegadores.

CSI 7.0 é uma solução de software para a gestão de vulnerabilidades de patches que se encarrega do processo completo de administração de patches. Integra a inteligência sobre as vulnerabilidades, rastreamento de vulnerabilidades e a criação de patches com uma ferramenta de implantação para fornecer uma gestão completa de patches confiáveis e rentáveis.

Para utilizar a console CSI 7.0, seu sistema deverá cumprir com os seguintes requisitos:

- Resolução mínima: 1024x768
- A última versão do Internet Explorer (os resultados de rastreamento podem ser visualizados em outros navegadores)
- Conexão com a Internet capaz de conectar-se à https://csi7.secunia.com
- Opção de cookies de origem ao menos configurada em Perguntar" (Prompt), em Internet Explorer
- Permitir a utilização de cookies na sessão
- Um leitor de PDF (por ex., Adobe Reader) – opcional

Capacidades de rastreamento e gerenciamento de patches de CSI 7.0

Para rastrear e criar atualizações de forma correta, os seguintes elementos deverão estar presentes quando utilizar CSI:

- Internet Explorer 8 ou posterior com o complemento do programa de instalação WSUS para CSI (somente para a console de administração)
- Visual C Runtime
- Microsoft .NET Framework 4 Runtime ou posterior
- Caso vá utilizar o certificado autofirmado de WSUS e o usuário quer fornecer através da função Patching (Gerenciamento de patches) > WSUS/SCCM > Deployment (Implementação), o serviço de registro remoto deverá estar habilitado nos equipamentos do cliente
- Selecione os hosts de destino onde deverá instalar o certificado (pressione CTRL+ enter para selecionar vários destinos), dê um clique direito e selecione Verify (Verificar) e Install Certificate (Instalar o certificado)
- O painel de controle proporciona uma visão geral dos hosts com a ajuda de vários "portlets". Os portlets são um grupo de componentes que apresentam dados chaves de forma gráfica e te permite criar perfis para apresentar uma combinação única de portlets.

DOWNLOAD E INSTALAÇÃO DO PLUGIN PARA CSI

A primeira vez que iniciar uma sessão em CSI, dê um clique no link na parte inferior da página e siga as instruções da tela para download e instale o complemento para CSI, ative o rastreamento e o aplicativo de patches. Considere que o complemento deve ser compatível com a última versão do Internet Explorer (deve ser executado utilizando o Internet Explorer).

O complemento para CSI deve ser instalado localmente na máquina em que a console CSI será executada. Uma vez que o complemento para CSI está instalado, o link de download será eliminado da página.

DOWNLOAD E INSTALAÇÃO DO DAEMON DE SECUNIA

O daemon de Secunia é um arquivo executável auto-sustentável que se encarrega do rastreamento e importa as tarefas programadas configuradas na console CSI. Se executa como serviço em segundo plano e não requer a interação do usuário. O download pode ser efetuado em daemon da Secunia.

O daemon da Secunia integra várias fontes de dados locais da rede com a núvem de Secunia. Deve ser implementado em um nó da rede que tenha uma alta disponibilidade (por ex., o servidor onde se executa SCCM ou servidor SQL). Uma vez implementado, o daemon rastreia as fontes de dados periodicamente baseando-se nas configurações criadas em CSI para as seguintes tarefas:

- Rastreamento do Active Directory
- Importação do SCCM (SQL + WSUS)
- Exportações programadas
- Mudanças de estado do WSUS

REQUISITOS DE RASTREAMENTO BASEADO NO AGENTE (PARA WINDOWS)

A flexibilidade que oferece CSI garante que seu ambiente se adaptará facilmente.

Se utiliza a instalação baseada em agente para concluir um rastreamento, os seguintes requisitos deverão estar presentes nos hosts de destino:

- Privilégios de administrador (para instalar o agente CSI: csia.exe) Microsoft Windows XP, 2003, 2008, Vista, 7 ou 8
- Conexão com a Internet: SSL 443/TCP para conectar-se a https://*.secunia.com/ Windows Update Agent 2.0 ou posterior

REQUISITOS DE RASTREAMENTO BASEADO NO AGENTE (PARA MAC OS X)

Deve contar com os seguintes requisitos antes de instalar o único agente para hosts em uma máquina Mac OS X baseada em Intel:

- Sistemas compatíveis: 10.5 Leopard/10.6 Snow Leopard/10.6 Snow Leopard Server/10.7 Lion/10.8 Mountain Lion
- Privilégios de administrador (requerem privilégios de 'raíz' para fazer a
- instalação)
- Conexão com a Internet: SSL 443/TCP para conectar-se a https://*. secunia.com
- O usuário que instala o agente deve ter permissões de execução para o arquivo (chmod +x)

REQUISITOS DE RASTREAMENTO REMOTO/ SEM AGENTE (PARA WINDOWS)

Caso prefira rastrear sem instalar o agente CSI (rastreamento sem agente), os requisitos que devem estar presentes no host de destino são os seguintes:

- Portas de entrada abertas: 139/TCP y 445/TCP (nos hosts)
- Compartilhamento de arquivos habilitado nos hosts
- Compartilhamento de arquivos simples desabilitado
- Windows Update Agent 2.0 ou posterior

Os seguintes serviços de Windows devem ser executados nos hosts:

- Serviços de estação de trabalho
- Serviços de servidor
- Serviços de registro remoto (está desabilitado no Win7/Vista de forma predeterminada)
- Serviços COM+ (Aplicação do sistema COM+: configurada Automaticamente)

RASTREAMENTO DO RED HAT ENTERPRISE LINUX (RHEL)

O agente de rastreamento para RHEL usa o inventário presente (RPM) e o apresenta em CSI, em seguida seu processamento é efetuado através das regras de detecção/versão do Secunia. Para download do agente CSI para Red Hat Linux, vá ao Scanning (Rastreamento) > Scanning via Local Agents (Rastreamento mediante agentes locais) > Download Local Agents (Download de agentes locais).

Aliança Tecnológica da ESET

O objetivo da Aliança tecnológica da ESET é oferecer a melhor proteção corporativa mediante uma série de soluções de segurança. Proporcionamos aos clientes uma opção melhor para o seu ambiente de segurança, que está em constante mudança, mediante a combinação de nossa tecnologia, confiança comprovada através do tempo e comparação com outros produtos da indústria nos destacamos como os melhores.

ENJOY SAFER TECHNOLOGY™