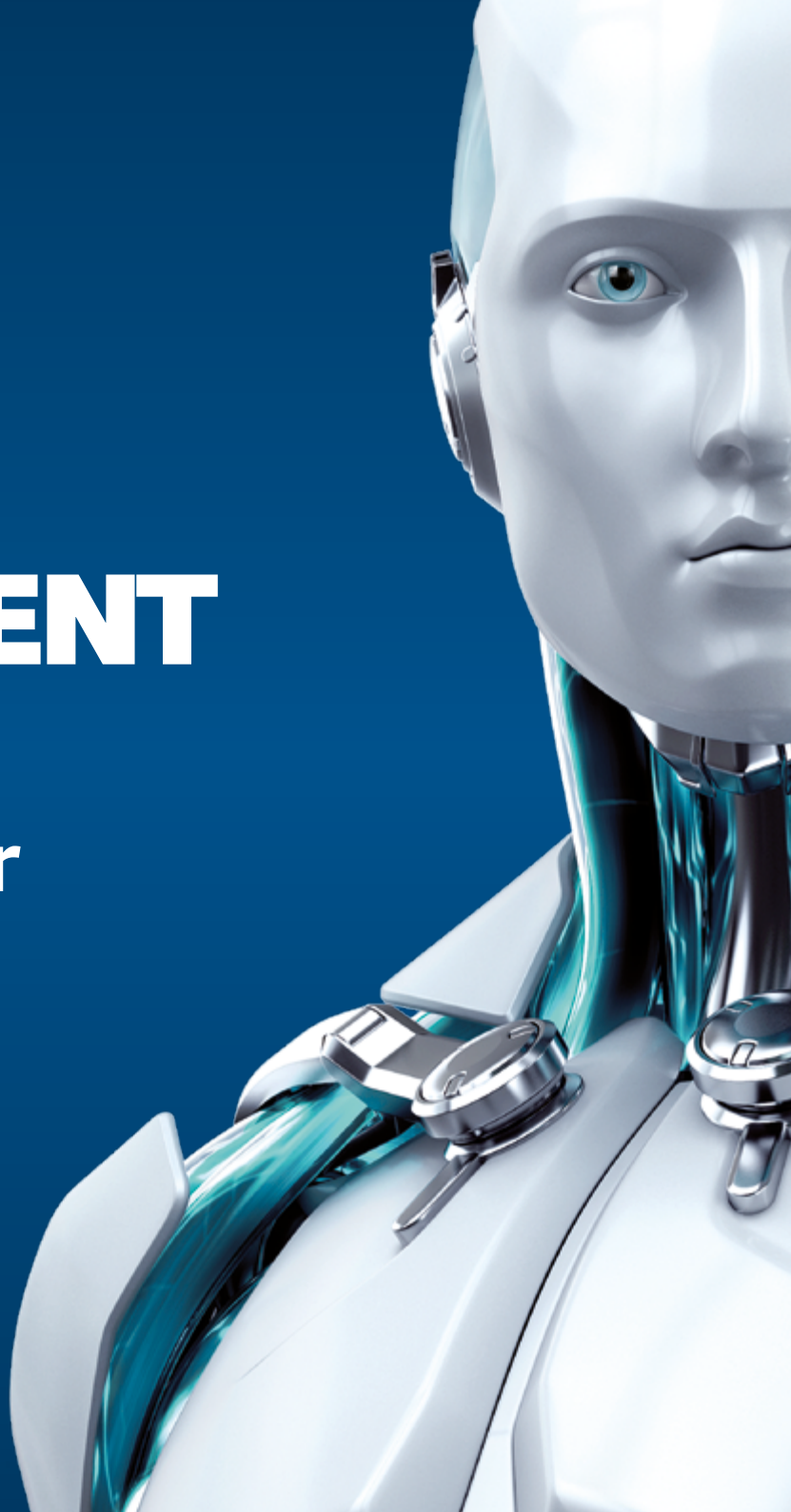
FLEXERA SOFTWARE

PATCH MANAGEMENT

Requisitos de sistema para Corporate Software Inspector



ESET TECHNOLOGY ALLIANCE

Flexera

Administración de parches con Corporate Software Inspector

Corporate Software Inspector gestiona el cuándo, dónde, qué y cómo de la instalación de parches de seguridad. Le avisa cuando hay un parche disponible para una vulnerabilidad de software que está amenazando su infraestructura, dónde tendrá el mayor impacto, qué estrategia de solución es la más adecuada y cómo implementarla.

Secunia Research verifica continuamente las vulnerabilidades y la eficacia de los parches publicados por los vendedores. Estos datos luego se adaptan a su infraestructura específica, por lo que es posible priorizar, planificar y ejecutar flujos de trabajo, así como documentar los esfuerzos para reducir riesgos.

REQUISITOS

Requisitos de sistema para Corporate Software Inspector (CSI) 7.0

CSI 7.0 es una solución basada en la Web. Es completamente funcional para usar con la última versión de Internet Explorer. Los resultados de las exploraciones también se pueden visualizar desde otros navegadores.

CSI 7.0 es una solución de software para la gestión de vulnerabilidades y parches que se encarga del proceso completo de administración de parches. Integra la inteligencia sobre vulnerabilidades, la exploración de vulnerabilidades y la creación de parches con una herramienta de despliegue para suministrar una gestión completa de parches confiable y rentable.

Para usar la consola CSI 7.0, su sistema deberá cumplir con los siguientes requisitos:

- Resolución mínima: 1024x768
- La última versión de Internet Explorer (los resultados de la exploración también se pueden visualizar desde otros navegadores)
- Conexión a Internet capaz de conectarse a https://csi7.secunia.com
- Opción de cookies de origen al menos configurada en „Preguntar" (Prompt), en Internet Explorer
- Permitir el uso de cookies de sesión
- Un lector de PDF (por ej., Adobe Reader) – opcional

Capacidades de exploración y gestión de parches de CSI 7.0

Para explorar y crear actualizaciones en forma correcta, los siguientes elementos deberán estar presentes cuando use CSI:

- Internet Explorer 8 o posterior con el complemento del programa de instalación WSUS para CSI (Solo para la consola de administración)
- Tiempo de ejecución de Visual C
- Tiempo de ejecución de Microsoft .NET Framework 4 o posterior
- Si se va a usar el certificado autofirmado de WSUS y el usuario quiere suministrarlo a través de la función Patching (Gestión de parches) > WSUS/SCCM > Deployment (Despliegue), el servicio de registro remoto deberá estar habilitado en los equipos cliente
- Seleccione los hosts de destino donde se deberá instalar el certificado (presione CTRL+ clic para seleccionar varios destinos), haga un clic derecho y seleccione Verify (Verificar) e Install Certificate (Instalar certificado)

El panel de control proporciona una vista general de los hosts con la ayuda de varios „portlets". Los portlets son un grupo de componentes que muestran datos claves en forma gráfica y le permiten crear perfiles para mostrar una combinación única de portlets.

DESCARGA E INSTALACIÓN DEL COMPLEMENTO PARA CSI

La primera vez que inicie sesión en CSI, haga clic en el enlace en la parte inferior de la página y siga las instrucciones en pantalla para descargar e instalar el complemento para CSI, y activar la exploración y la aplicación de parches. Tenga en cuenta que el complemento es compatible con la última versión de Internet Explorer (es decir, se debe ejecutar utilizando Internet Explorer).

El complemento para CSI se debe instalar localmente en la máquina donde se está ejecutando la consola CSI. Una vez que el complemento para CSI está instalado, el enlace de descarga se elimina de la página.

DESCARGA E INSTALACIÓN DEL DAEMON DE SECUNIA

El daemon de Secunia es un archivo ejecutable autosostenible que se encarga de la exploración e importa las tareas programadas configuradas en la consola CSI. Se ejecuta como servicio en segundo plano y no requiere la interacción del usuario. Desde aquí puede descargar el daemon de Secunia.

El daemon de Secunia integra varias fuentes de datos locales de la red con la nube de Secunia. Debe desplegarse en un nodo de la red que tenga una alta disponibilidad (por ej., el servidor donde se ejecuta SCCM o el servidor SQL). Una vez desplegado, el daemon explorará las fuentes de datos periódicamente basándose en las configuraciones creadas en CSI para las siguientes tareas:

- Exploración de Active Directory
- Importación de SCCM (SQL + WSUS)
- Exportaciones programadas
- Cambios de estado de WSUS

REQUISITOS DE LA EXPLORACIÓN BASADA EN AGENTE (PARA WINDOWS)

La flexibilidad que ofrece CSI garantiza que se adaptará fácilmente a su entorno.

Si usa la instalación basada en agente para llevar a cabo la exploración, los siguientes requisitos deberán estar presentes en los hosts de destino:

- Privilegios de administrador (para instalar el agente CSI: csia.exe) Microsoft Windows XP, 2003, 2008, Vista, 7 u 8
- Conexión a Internet: SSL 443/TCP para conectarse a https://*.secunia.com/ Windows Update Agent 2.0 o posterior

REQUISITOS DE LA EXPLORACIÓN BASADA EN AGENTE (PARA MAC OS X)

Debe contar con los siguientes requisitos antes de instalar el agente único para hosts en una máquina Mac OS X basada en Intel:

- Sistemas compatibles: 10.5 Leopard/10.6 Snow Leopard/10.6 Snow Leopard Server/10.7 Lion/10.8 Mountain Lion
- Privilegios de administrador (se requieren privilegios de 'raíz' para hacer la instalación)
- Conexión a Internet: SSL 443/TCP para conectarse a https://*.secunia.com
- El usuario que instala el agente debe tener permisos de ejecución para el archivo (chmod +x)

REQUISITOS DE LA EXPLORACIÓN REMOTA/SIN AGENTE (PARA WINDOWS)

Si en cambio prefiere explorar sin instalar el agente CSI (exploración sin agente), los siguientes son los requisitos que deberán estar presentes en los hosts de destino:

- Puertos entrantes abiertos: 139/TCP y 445/TCP (en los hosts)
- Uso compartido de archivos habilitado en los hosts
- Uso compartido simple de archivos deshabilitado
- Windows Update Agent 2.0 o posterior

Los siguientes servicios de Windows se deben estar ejecutando en los hosts:

- Servicio de estación de trabajo
- Servicio de servidor
- Servicio de registro remoto (está deshabilitado en Win7/Vista en forma predeterminada)
- Servicios COM+ (Aplicación del sistema COM+: configurada en Automático)

EXPLORACIÓN DE RED HAT ENTERPRISE LINUX (RHEL)

El agente de exploración para RHEL usa el inventario presente (RPM) y lo muestra en CSI luego de su procesamiento por las reglas de detección/versión de Secunia. Para descargar el agente CSI para Red Hat Linux, vaya a Scanning (Exploración) > Scanning via Local Agents (Exploración mediante agentes locales) > Download Local Agents (Descargar agentes locales).

Alianza Tecnológica de ESET

El objetivo de la Alianza tecnológica de ESET es mejorar la protección corporativa mediante una serie de soluciones de seguridad informática. Les proporcionamos a los clientes una mejor opción en el entorno de seguridad, que se halla en cambio constante, mediante la combinación de nuestra tecnología de confianza comprobada por el tiempo con otros productos que constituyen los mejores en su campo.

ENJOY SAFER TECHNOLOGY™