Ivanti Neurons Patch for MEM (Microsoft Endpoint Manager)

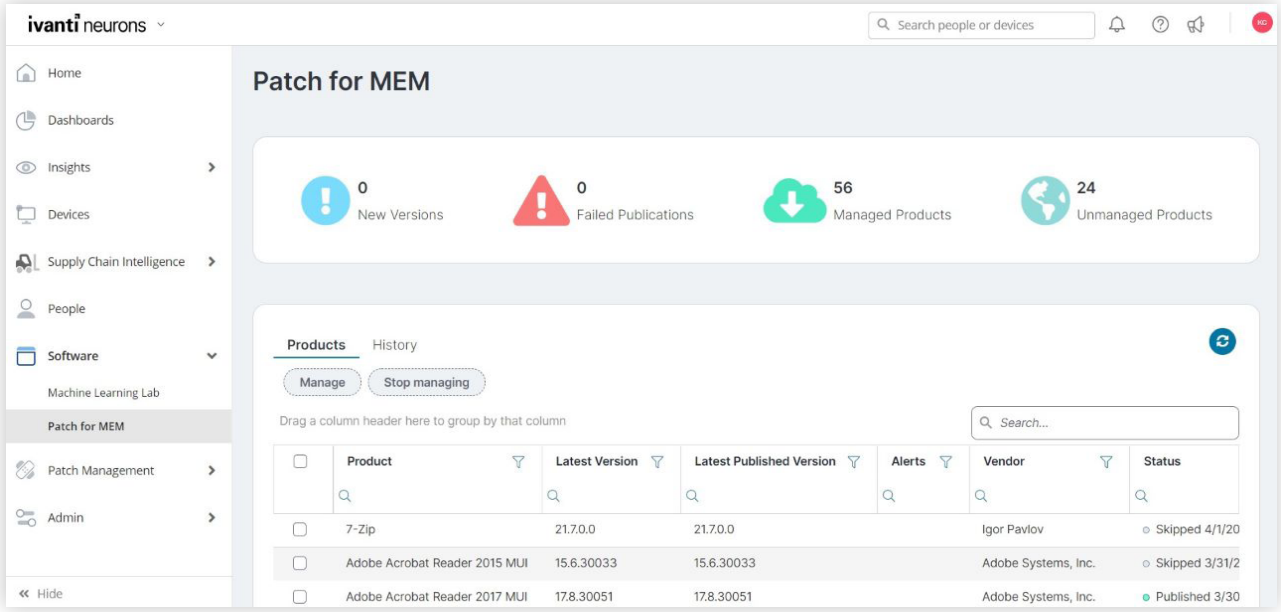
Amplíe Microsoft Intune con la publicación de parches de terceros basadas en el riesgo

Ivanti Neurons Patch for MEM amplía las implementaciones existentes de Microsoft Intune para incluir las actualizaciones de aplicaciones de terceros. Su información sobre parches y amenazas ayuda a las empresas a priorizar adecuadamente la reparación de vulnerabilidades de software de terceros.

Actualizaciones de terceros en Intune

Las violaciones de datos y los ataques de ransomware son cada vez más frecuentes. Del mismo modo, el número de aplicaciones que despliegan las empresas también está en aumento, un 24 % desde 2016.[1] Por consiguiente, no debería sorprender que las aplicaciones de terceros se hayan convertido en uno de los vectores de ataque más atractivos para los ciberdelincuetes. Lamentablemente, las violaciones de datos derivadas de las vulnerabilidades de las aplicaciones de terceros también se encuentran entre las más caras, ya que cuestan a las empresas una media de 4,33 millones de dólares.[2]

Por ese motivo, las empresas deben ser diligentes a la hora de actualizar las aplicaciones de terceros, lo que puede suponer un reto con el número cada vez mayor de aplicaciones que deben tener en cuenta. Para complicar aún más la situación, el número de vulnerabilidades que hay que controlar es cada vez mayor: la Base de Datos Nacional de Vulnerabilidades (NVD) revela una media de 61 cada día.[3]



La buena noticia es que solo el 4 % de todas las Vulnerabilidades y Exposiciones Comunes (CVEs) se han explotado públicamente.[4] La mala noticia es que identificar ese 4 % de las más de 130.000 vulnerabilidades totales en el NVD, puede ser difícil. Por ejemplo, si una empresa tuviera que parchear todas las vulnerabilidades críticas basadas en el Sistema de Puntuación de Vulnerabilidad Común (CVSS) v3, dejaría de parchear el 73,61 % de las vulnerabilidades de ransomware o secuestro de datos.[3]

Esta situación puede ser aún más problemática para las empresas que aprovechan Microsoft Intune para entregar aplicaciones y actualizaciones a sus dispositivos. Mientras que Intune ofrece amplias capacidades de gestión de parches para las aplicaciones de Microsoft, no proporciona ninguna funcionalidad nativa para la actualización de aplicaciones de terceros.

Introducción a Ivanti Neurons Patch for MEM

Ivanti Neurons Patch for MEM amplía las implementaciones existentes de Microsoft Intune para incluir capacidades de actualización de aplicaciones de terceros sin necesidad de ninguna infraestructura adicional. También proporciona información sobre amenazas y fiabilidad de los parches para que los equipos de TI prioricen y corrijan las vulnerabilidades que suponen un mayor riesgo para su compañía. Con Ivanti Neurons Patch for MEM, las empresas pueden protegerse mejor de las filtraciones de datos, el ransomware y otras amenazas derivadas de las vulnerabilidades de las aplicaciones de terceros.

Características y capacidades principales

Ampliar Microsoft Intune con publicaciones de parches de terceros

Maximice el rendimiento de su inversión en Intune a la vez que se protege contra las amenazas derivadas de las vulnerabilidades de las aplicaciones de terceros. Ivanti Neurons Patch for MEM publica actualizaciones de aplicaciones de terceros previamente probadas desde la plataforma en la nube Neurons de Ivanti, directamente en Intune. Esto permite a los equipos de TI implementar actualizaciones de aplicaciones de terceros junto con las actualizaciones de aplicaciones y del sistema operativo de Microsoft dentro de Intune, como parte de sus flujos de trabajo de gestión del ciclo de vida de las aplicaciones existentes.

Los clientes de Intune pueden migrar sus cargas de trabajo de parcheo completamente a la nube, y disfrutar de la visión de gestión moderna de Microsoft sin ninguna infraestructura adicional.

Protéjase proactivamente contra los exploits activos

Dé prioridad a la corrección en función del riesgo de los adversarios con información sobre los exploits conocidos y el contexto de las amenazas para las vulnerabilidades, incluidos los vínculos con el ransomware. La Calificación de Riesgo de Vulnerabilidad (VRR) de Ivanti le permite adoptar medidas prioritarias basadas en el riesgo, mejor que la calificación básica de CVSS, ya que tiene en cuenta los datos de vulnerabilidad y amenaza de mayor fidelidad, además de la validación humana de los exploits por parte de los equipos de pruebas de penetración.

Ahorre tiempo y evite despliegues de parches fallidos con actualizaciones de aplicaciones previamente probadas y datos de fiabilidad. Ivanti prueba a fondo cada paquete de contenido de parches que creamos. Las pruebas se realizan en un extenso entorno virtual, para garantizar que los paquetes funcionan en una amplia gama de versiones de aplicaciones y sistemas operativos antes de que se lancen al producto.

Para reforzar aún más su confianza, la información de fiabilidad de los parches procedente de datos colaborativos de percepción social y telemetría de despliegue de parches anonimizada, le permite evaluar las actualizaciones de aplicaciones según su fiabilidad en entornos del mundo real previo a su implantación.

Agilizar los procesos de gestión de parches

Consiga una eficacia operativa en diversos ámbitos gracias a las útiles funciones de Ivanti Neurons Patch for MEM:

- Publique automáticamente actualizaciones de terceros en tiempo real, a medida que se van haciendo disponibles (autopublicación opcional).
- Consiga una aplicación de parches más fiable y con menos fallos al aprovechar las actualizaciones de aplicaciones previamente probadas junto con la información sobre la fiabilidad de los parches.
- Priorice de manera efectiva los esfuerzos de parcheo con la inteligencia de amenazas, para que pueda enfocarse en lo que realmente le importa.
- Facilite las conversaciones sobre datos y riesgos entre los equipos de seguridad y operaciones de TI con información sobre exploits y malware para mejorar la colaboración operativa.

Sobre Ivanti

Ivanti hace que sea posible trabajar desde “cualquier lugar”. En el teletrabajo, los empleados utilizan un sinfín de dispositivos para acceder a las redes y aplicaciones de TI, y a los datos a través de varias redes para seguir siendo productivos mientras trabajan desde cualquier lugar. La plataforma de automatización Ivanti conecta las soluciones líderes del sector de gestión unificada de dispositivos, seguridad de confianza cero y gestión de servicios empresariales, proporcionando un panel único para que las empresas puedan autocurar y autoproteger los dispositivos, y autoservir a los usuarios finales. Más de 40.000 clientes, entre los que se encuentran 96 de las 100 empresas de la lista Fortune, han optado por Ivanti para descubrir, gestionar, proteger y dar servicio a sus activos de TI desde la nube hasta el terminal, y ofrecer excelentes experiencias de usuario final a los empleados, dondequiera y comoquiera que trabajen. Para más información, visite ivanti.es.

ivanti

ivanti.es
+34 91 049 66 76
contact@ivanti.es

1. Okta, “Business at Work 2022 Report”, 2022. https://www.okta.com/report/businesses-at-work-2022/
2. IBM Security, “2021 Cost of a Data Breach Report”, 28 de julio de 2021. https://www.ibm.com/security/data-breach
3. Cyber Security Works, Cyware, Ivanti, “2022 Ransomware Spotlight Report”, 26 de enero de 2022. https://www.ivanti.com/lp/security/reports/ransomware-spotlight-year-end-2021-report
4. Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA), “Binding Operational Directive 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities”, 3 de noviembre de 2021. https://cyber.dhs.gov/bod/22-01/