pandasecurity.com/business/

Patch Management

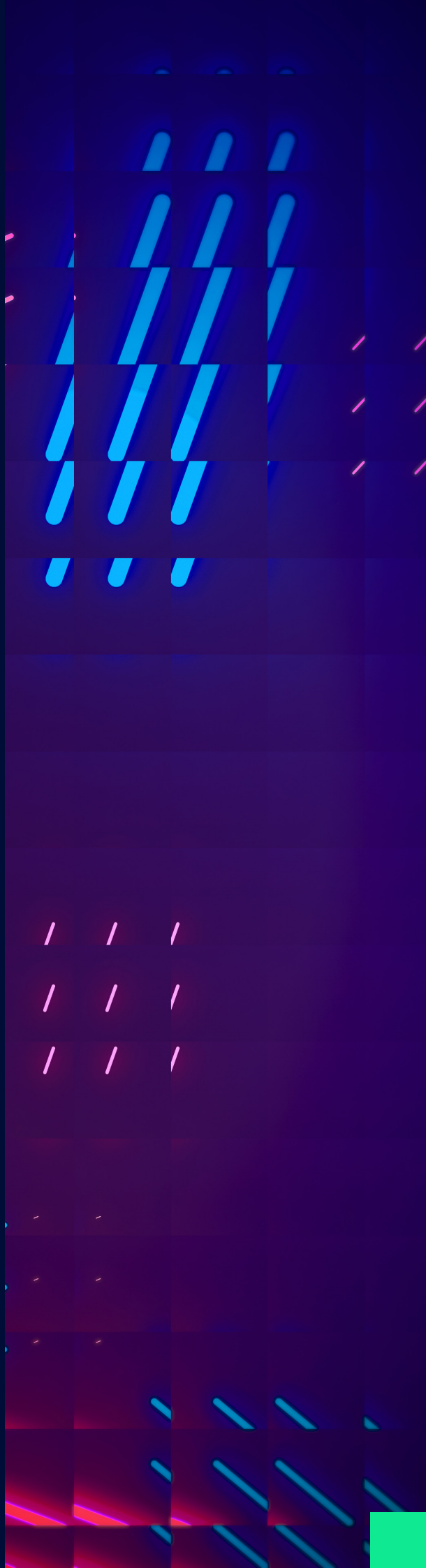
Índice:

1. La importancia de la gestión de parches en las organizaciones
2. Las vulnerabilidades en números
3. Vulnerabilidades conocidas; vulnerabilidades de alto riesgo
4. Gestión de parches
5. Ciclo de vida de la gestión de parches
6. Mantén las vulnerabilidades conocidas fuera de tu infraestructura IT con Panda Patch Management

|La importancia de la gestión de parches en las organizaciones

Los parches de software tienden a ser una molestia para los administradores IT debido a que su priorización y despliegue es una tarea costosa, y también para los usuarios, ya que en algunos casos requiere invertir tiempo en reiniciar equipos y servidores lo que a menudo implica interrupciones en su trabajo. Por ello, normalmente acabamos posponiendo su actualización y los parches recomendados acaban siendo ignorados. Sin embargo, lo que parece una acción inocente puede acabar teniendo graves consecuencias para las organizaciones.

De las misma manera, los administradores IT pueden tener serias dificultades para garantizar que todos los sistemas de su parque tengan los parches adecuados instalados. Los parches y actualizaciones de software son algo crítico a la hora de mantener una organización madura en términos de ciberseguridad, ya que evitan que el software y los sistemas sean vulnerables ante amenazas de seguridad.



panda

|Las vulnerabilidades en números

El número de vulnerabilidades de seguridad reportadas en 2018 fue de **16.556**, por eso no es de extrañar que sea extremadamente complicado para una organización con recursos de IT limitados, mantener y proteger su infraestructura.

La administración de parches es una tarea que precisa tiempo y recursos, y a menudo es difícil tener una visión global de las aplicaciones y los activos, priorizar los parches e incluso disponer de la capacidad para que puedan parchearse programas y sistemas críticos rápidamente. Para las empresas es clave realizar esta gestión de parches de la forma más eficaz posible, ya que de no ser así, su impacto puede tener efectos muy negativos en términos económicos y de ciberseguridad.

El 24.1%[1] de las vulnerabilidades pertenece a cinco compañías: Software en el Interés Público (SPI), SUSE, Oracle, IBM y Microsoft.

Las aplicaciones de terceros más utilizadas son los principales objetivos de los hackers. De acuerdo con el índice de vulnerabilidades y exposiciones comunes (CVE[2]), aplicaciones como Java, Adobe, Google Chrome, Mozilla Firefox, y OpenOffice entre otras, son las que mayor número de vulnerabilidades presentan, por lo que parchear únicamente los sistemas operativos no es suficiente.

Otro factor a tener en cuenta es el incremento del número de atacantes que tienen las habilidades necesarias para descubrir vulnerabilidades a una mayor velocidad. Una vez las encuentran, implementan programas de ataque que automatizan la explotación de estas nuevas vulnerabilidades, siendo además, ampliamente distribuidos, a veces incluso se hacen virales. El resultado de esta combinación de amenazas, vulnerabilidades y consecuencias supone un riesgo significativo para las empresas, pero por sorprendente que parezca, no son las vulnerabilidades que están aún por descubrir las que mayor peligro conllevan.

Fuentes:
1. Cybersecurity alert – TechRepublic
2. attack.mitre.org – MITRE

|Vulnerabilidades conocidas; vulnerabilidades de alto riesgo

En la actualidad, las vulnerabilidades y su explotación siguen siendo la causa principal de la mayor parte de las brechas de seguridad, aún recordamos los casos de **WannaCry, Petya o BlueKeep** que causaron estragos a nivel mundial. Solo un reducido número de ataques se producen como consecuencia de una vulnerabilidad desconocida (ataques de día cero), ya que la mayoría provienen de vulnerabilidades conocidas.

Según Gartner[3], el 99% de las vulnerabilidades explotadas a finales de 2020 continuarán siendo conocidas por los profesionales de seguridad y administradores IT en el momento del incidente. Por el contrario, las vulnerabilidades de día cero han supuesto aproximadamente el 0,4% de las vulnerabilidades durante la última década.

Además, hay que tener en cuenta que los hackers disponen de exploits públicos para perpetrar sus ataques y no dudan en aprovecharlos sabiendo que la mayoría de las empresas no parchean sus sistemas. De hecho, el 80% de los ataques realizados con éxito se aprovechan de vulnerabilidades con parches conocidos pero que no han sido aplicados.

Antes estos hechos, resulta obvio que las empresas debamos enfocar nuestros esfuerzos en controlar y mitigar las vulnerabilidades conocidas que se explotan repetidamente, ya que suponen un riesgo más real y mayor que los producidos por otros tipos de amenazas.

El espacio de tiempo transcurrido entre la revelación de una vulnerabilidad y su explotación se ha acortado, obligando a las empresas a ir a contrarreloj para desplegar un parche antes de que los cibercriminales puedan comprometer sus sistemas utilizando distintos vectores de ataque.

> El 57% de las víctimas de ciberataques declaran que la aplicación de un parche habría evitado el ataque. El 34% dice que conocía la vulnerabilidad antes del ataque[4].

Fuentes:
3. Focus on the Biggest Security Threats, Not the most Publicized – Gartner
4. Cost and consequences of gaps in vulnerability response – Ponemon

|Gestión de parches

a) En qué consiste

Es el proceso mediante el cual las organizaciones y en concreto sus departamentos IT descargan, prueban e instalan parches (cambios en el código o los datos) destinados a actualizar, optimizar o asegurar el software en equipos, servidores y sistemas con el objetivo de mantener su operatividad o mitigar las vulnerabilidades de seguridad. Aunque, parezca algo simple de realizar, la mayoría de las empresas luchan por identificar qué actualizaciones críticas de parches necesitan probar e instalar primero, de ahí, que la priorización de los parches sea clave para los administradores. De hecho, según Ponemon el promedio de tiempo empleado por las empresas para parchear aplicaciones o sistemas es de 102 días[5]. Sin embargo, de media transcurren 43 días[6], hasta que vemos el primer ataque que utiliza una vulnerabilidad critica de seguridad desde la publicación del parche por lo que existe un **gap de riesgo** de **59 días** de promedio.

Fuentes:
5. State of Endpoint security risk 2018 – Ponemon
6. Cost and consequences of gaps in vulnerability response – Ponemon

Existen diferentes tipos de parches, y cada uno es desarrollado para un fin concreto; corregir un error o vulnerabilidad específica. Estos son algunos ejemplos: Hotfix, parche o lanzamiento puntual, versión de mantenimiento, parches no oficiales, Monkey patches, etc.

En este documento nos fijamos en los dos que consideramos más importantes, ya que su objetivo es corregir vulnerabilidades críticas de seguridad conocidas, que son las más populares y explotadas por los atacantes y, por tanto, las más determinantes para las empresas y expertos en seguridad:

- **Parches de seguridad** - **afectan tanto a Sistemas Operativos como a Software de Terceros):** un parche de seguridad es un cambio aplicado a una aplicación o programa para corregir la debilidad descrita por una vulnerabilidad. Esta acción correctiva evita la posible explotación y eliminará o mitigará la capacidad de una amenaza para explotar una vulnerabilidad específica en un activo. La administración de parches es parte de la gestión de vulnerabilidades: la práctica cíclica de identificar, clasificar, remediar y mitigar vulnerabilidades (riesgos de seguridad).

- **Service Pack (SP)** o **Feature Pack (FP):** son parches importantes que comprenden una colección de actualizaciones, correcciones o mejoras de funciones para un programa de software, estos suelen solucionar muchos problemas pendientes y normalmente incluyen todos los parches, revisiones, parches de mantenimiento y seguridad lanzados antes del Service Pack.

b) Cuál es su propósito

Los parches están diseñados para reparar una vulnerabilidad o agujero de seguridad identificado después del lanzamiento de una aplicación o software.

El software no parcheado puede hacer que los endpoints sean un objetivo vulnerable ante exploits, suponiendo una gran oportunidad para que los hackers puedan realizar un ataque con éxito. Los parches de software son un componente crítico de las operaciones y la seguridad para los administradores y expertos en seguridad.

En el sector tecnológico y concretamente en el del software, suele ser habitual que, una vez desarrollada una aplicación exista la necesidad de tener que actualizarla, corregirla o incluso modificarla. Por esta razón, es aconsejable desarrollar un proceso similar al del ciclo de vida del software en el que se distingan diferentes fases que permitan el análisis, la evaluación y la aplicación de parches de forma regular y así solucionar los problemas que pudieran ocasionar.

|Ciclo de vida de la gestión de parches

La administración de parches puede ser la herramienta más efectiva utilizada para proteger tu empresa de las vulnerabilidades y la menos costosa de mantener si se implementa de manera eficiente. En este apartado, describimos como establecer un procedimiento de gestión de parches de rutina con el objetivo de hacer que forme parte de las operaciones estándar de tu empresa. En este ciclo o procedimiento diferenciamos seis fases[7]:

Identificación de activos y software base:

la identificación de activos y su software base instalado, así como el nivel de parches, es una tarea compleja pero que mejora la seguridad y la operación. Disponer de esta base permite llevar a cabo cambios en el sistema sin riesgos y posibilita volver a un estado previo conocido y funcional en caso de producirse algún problema a la hora de instalar una actualización o parche.

Disponibilidad:

En función del inventario de activos y el software identificado, se ha de revisar el listado de parches actual e identificar cuál de ellos afecta a cada activo del proceso.

Aplicabilidad:

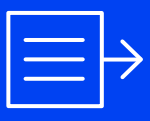
Los parches publicados no siempre son válidos para todos los dispositivos, por lo que se ha de verificar si esa actualización concreta es apta para los activos de nuestro proceso.

Adquisición:

Obtener los ficheros de actualización de una fuente oficial, así como comprobar la veracidad del parche no siempre es fácil. La utilización de hashes no es habitual para los parches relacionados con los sistemas de control.

Validación:

El objetivo de la validación es asegurar que la actualización no impacte negativamente en el proceso. Para llevarla a cabo, se han de utilizar activos de pruebas y seguir las fases de despliegue. Con la validación se pretende comprobar las implicaciones de la actualización, que puede incluir cambios en las políticas del cortafuegos, modificaciones de configuración, etc.



Despliegue:

Durante el proceso de validación se deberá crear un paquete de despliegue. El paquete debe contener los ficheros de actualización y las instrucciones para su instalación, así como un listado de los activos en los realizar el despliegue.

Fuentes:
7. Gestión de parches en sistemas de control – INCIBE-CERT

|Mantén las vulnerabilidades conocidas fuera de tu infraestructura IT con Panda Patch Management

Panda Patch Management, es una solución que consigue hacer simple el complejo ciclo de vida de gestión de parches de sistemas operativos y software de terceros. El resultado es una reducción de la superficie de ataque, fortaleciendo las capacidades preventivas, y de contención ante incidentes por vulnerabilidades en los sistemas.

La solución, que no requiere de nuevos agentes ni consola de gestión propia al estar integrada en las soluciones de seguridad endpoint de Panda Security, proporciona visibilidad en tiempo real y centralizada del estado de las vulnerabilidades, parches, actualizaciones pendientes, y software no soportado o en EoL (End-of-Life) en los equipos y servidores localizados tanto dentro como fuera de la red corporativa. Sus herramientas de gestión permiten en tiempo real, automatizar el descubrimiento, la planificación, la instalación y la monitorización de parches y actualizaciones críticos para tu organización de una forma extremadamente simple e intuitiva.

Entre los principales beneficios y características que Panda Patch Management aporta se encuentran:

- Capacidad para **auditar, monitorizar y priorizar** las **actualizaciones** de los sistemas operativos y aplicaciones. Permite ver el estado de los parches y actualizaciones pendientes del sistema y de cientos de aplicaciones de terceros, e incluso hacer rollback de parches.
- **Prevención de incidentes,** reduciendo sistemáticamente la superficie de ataque por vulnerabilidades. La gestión de parches y actualizaciones permite adelantarse a la explotación de vulnerabilidades.
- **Contener y mitigar ataques que explotan vulnerabilidades,** aplicando inmediatamente las actualizaciones críticas desde la consola cloud. La consola correlaciona detecciones con vulnerabilidades, minimizando así el tiempo de respuesta, contención y remediación mediante la actualización necesaria desde la consola. Adicionalmente, permite aislar de la red los equipos afectados, conteniendo el ataque o potencial ataque.
- **Reducción de los costes operativos**, al no requerir despliegues ni actualizaciones de agente en los endpoints, **simplificando la gestión** sin sobrecargar los equipos y servidores. **Minimiza el esfuerzo de las actualizaciones remotas** desde la consola cloud. **Visibilidad inmediata** y desatendida de vulnerabilidades, actualizaciones y aplicaciones en EoL.

La gestión de parches es un proceso que debe realizarse de manera rutinaria y ser lo más completo posible para ser eficaz. Esto, no quiere decir que todos los sistemas deban ser tratados por igual; cada empresa debe priorizar sus activos y proteger primero los más críticos. Dicho esto, es importante asegurar que los parches se desplieguen en todas las máquinas y no solo en las más valiosas o importantes para la empresa. Además, los parches no solo requerirán el esfuerzo de los administradores del sistema, sino que también pueden requerir el apoyo de la empresa para acordar una ventana de mantenimiento específica.

Protección de ataques

Arquitectura de seguridad adaptativa

Predecir/ Anticiparse

Descubrimiento de vulnerabilidades, parches, actualizaciones pendientes y aplicaciones en EoL.

Prevenir

Automatizar el parcheo planificado. Reemplazar las aplicaciones en EoL.

Responder

Parcheo de todas las aplicaciones vulnerables.

Detectar y Contener

Contención de ataques mediante el parcheo en tiempo real.

Descubre como Panda Patch Management puede ayudarte a simplificar la gestión de las vulnerabilidades a través de la administración de actualizaciones y parches de seguridad.

Solicita una Demo/Trial

Contacta con nosotros*

Nombre
000 000 000
email@pandasecurity.com

panda