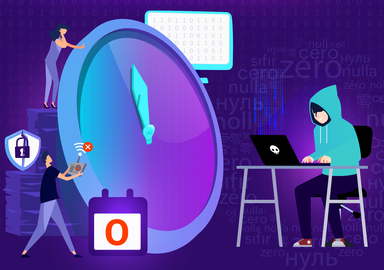
ManageEngine
Vulnerability Manager Plus

ZERO-DAY 101



DESCIFRANDO LOS ATAQUES DE DÍA CERO

Vulnerabilidades de día cero → **Exploits de día cero** → **Ataques de día cero**

¿Qué es una vulnerabilidad de día cero?

Es una falla misteriosa en el software que surge sin el conocimiento del proveedor. Estas vulnerabilidades de seguridad no tienen parches disponibles de inmediato.

¿Por qué usamos este nombre?

Las organizaciones implementan parches de día cero para proteger sus sistemas de este tipo de vulnerabilidades, y los proveedores tienen "cero días" para desarrollar los parches necesarios. Sin una estrategia de mitigación adecuada, esta vulnerabilidad puede convertirse en un ciberataque grave.

¿Qué son los ataques de día cero?

Un ataque de día cero ocurre cuando se explota una vulnerabilidad de día cero debido a la falta de parches disponibles.

¿Cómo se previenen las vulnerabilidades de día cero?

1. Asegurarse de tener escáneres de vulnerabilidades activos
2. Instalar los parches aplicables de manera oportuna
3. Contar con un plan de mitigación provisional disponible

¿Por qué se consideran peligrosos los exploits de día cero?

Fallos ocultos: Estas vulnerabilidades pueden ser explotadas durante mucho tiempo antes de ser descubiertas.

Polimórficos: El malware generado por exploits de día cero puede adaptarse para atacar continuamente y evadir la detección.

Penetrativo: Un ataque de día cero puede infiltrarse en múltiples sistemas dentro de una red.

ATAQUES DE DÍA CERO QUE DEJARON UN IMPACTO SIGNIFICATIVO EN 2023

ATAQUE DE DÍA CERO EN WORDPRESS

Un exploit de día cero en un plugin con 200,000 usuarios permitió a los hackers evadir protecciones y obtener privilegios administrativos.

Fuente: SecurityWeek

CRIPTOMONEDAS ROBADAS POR UNA ÚNICA VULNERABILIDAD DE DÍA CERO

Aproximadamente 1.6 millones en criptomonedas fueron robados debido a un exploit de día cero en los cajeros automáticos de Bitcoin de General Bytes.

Fuente: TheHackerNews

ATAQUE A HITACHI ENERGY POR RANSOMWARE DEBIDO A UNA VULNERABILIDAD CRÍTICA DE DÍA CERO

La vulnerabilidad de día cero se encontró en un software de terceros utilizado por la banda de ransomware CLOP, que robó datos de los servidores en la nube de la organización.

Fuente: BleepingComputer

VULNERABILIDADES DE DÍA CERO SOLUCIONADAS POR PROVEEDORES RECONOCIDOS EN EL PRIMER SEMESTRE DE 2023

Número de vulnerabilidades de día cero solucionadas en **Chrome**

10

Número de vulnerabilidades de día cero solucionadas **Microsoft**

55

¿LA SOLUCIÓN PARA DETECTAR Y MITIGAR VULNERABILIDADES DE MANERA EFICIENTE?

ManageEngine Vulnerability Manager Plus revoluciona la detección de vulnerabilidades al identificar rápidamente las vulnerabilidades de día cero y mitigarlas con soluciones alternativas, antes de que sean explotadas.

DESCARGA AHORA

Protege tus endpoints, previene ciberataques