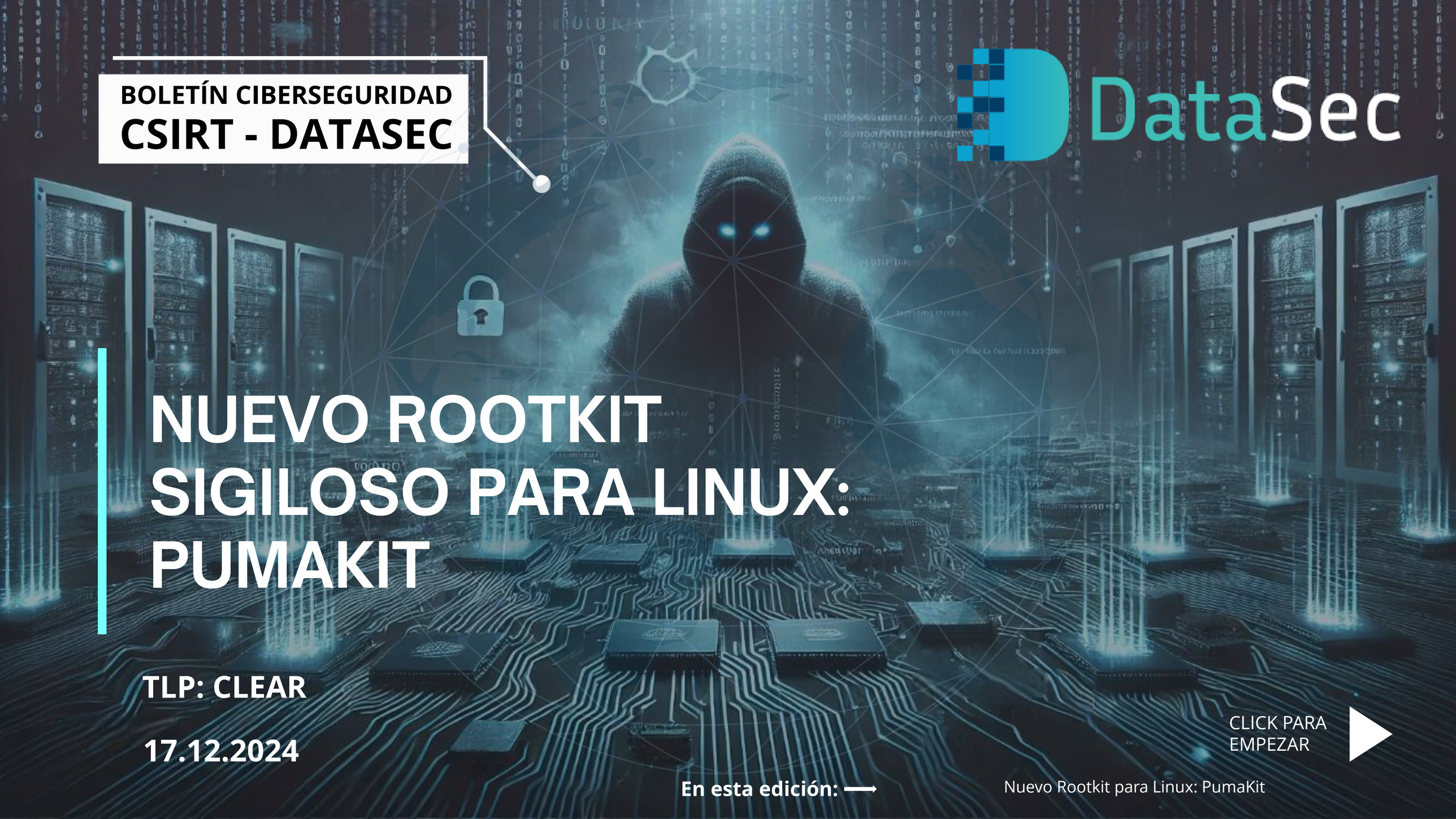


BOLETÍN CIBERSEGURIDAD
CSIRT - DATASEC

DataSec

NUEVO ROOTKIT SIGILOSO PARA LINUX: PUMAKIT

TLP: CLEAR

17.12.2024

CLICK PARA EMPEZAR

En esta edición:

CONTENIDO

DataSec

- Nuestra Esencia
- Vulnerabilidades
- Noticias
- Recomendaciones

NUESTRA ESENCIA

BOLETÍN CIBERSEGURIDAD

Este boletín está diseñado para mantener al lector informado y brindarle pautas de seguridad en un entorno digital en constante evolución. Incluye contenido sobre las últimas amenazas, vulnerabilidades y las mejores prácticas de protección.

EMPRESA

DataSec es una empresa colombiana líder en servicios tecnológicos, enfocada en la implementación, administración, soporte, monitoreo y gestión de plataformas de Seguridad Informática y Networking, con años de experiencia en proyectos de ciberseguridad y conectividad para diversos sectores.

SOC

DataSec cuenta con un Centro de Operaciones de Seguridad Cibernética (CSOC) especializado en la detección, análisis y respuesta a amenazas. Este centro opera de manera continua 24/7, contribuyendo a la prevención y mitigación de incidentes en tiempo real.

Cisco NX-OS Software Image Verification Bypass Vulnerability

CVE-2024-20397

Medium (5.2)

Impacto: Acceso no autorizado.

Resumen: Una vulnerabilidad en el gestor de arranque de Cisco NX-OS permite a un atacante con acceso físico o local con privilegios administrativos eludir la verificación de la firma de la imagen del sistema, explotando configuraciones inseguras del bootloader para cargar software no verificado.

Productos Afectadas

- Conmutadores multicapa de la serie MDS 9000.
- Conmutadores Nexus serie 3000 .
- Conmutadores Nexus serie 7000.
- Entre otros *Ver +INFO.*

Solución: Cisco ha publicado actualizaciones de software gratuitas que solucionan la vulnerabilidad descrita en este aviso.
Ver +INFO.

Fecha de Publicación: 04/DIC/2024

Tenable - Security Center Version Multiple Vulnerabilities

CVE-2024-5458, CVE-2024-5585, CVE-2024-4603
CVE-2024-4741, CVE-2024-5535, CVE-2024-6119
CVE-2023-49582, CVE-2024-12174

Critical (9.8)

Impacto: Intervención de correos.

Resumen: Se identificaron vulnerabilidades en componentes de terceros de Tenable Security Center y una falla en la validación de certificados, que podría permitir a un atacante interceptar correos mediante un servidor SMTP malicioso.

Versiones Afectadas

Security Center versiones anteriores a 6.5.0.

Solución: Tenable ha lanzado Security Center 6.5.0 para solucionar estos problemas. Los archivos de instalación se pueden obtener en el portal de descargas de Tenable.
Ver +INFO.

Fecha de Publicación: 05/DIC/2024

Veeam Service Provider Console Vulnerabilities

CVE-2024-42448, CVE-2024-42449

Critical (9.9)

Impacto: Ejecución de código arbitrario.

Resumen: Se identificaron vulnerabilidades en VSPC que permiten, desde la máquina del agente de gestión autorizado, ejecutar código remoto (RCE), filtrar hashes NTLM de la cuenta de servicio y eliminar archivos en el servidor afectado.

Versiones Afectadas

- Service Prov Console 8 – Versión 8.1.0.21377 y anteriores.
- Service Prov Console 7 – Todas las versiones.

Solución: Consultar la sección de Solución en el link del fabricante para obtener más correcciones de las versiones de mantenimiento y más utilizadas. *Ver +INFO.*

Fecha de Publicación: 05/DIC/2024

Vulnerabilidad de severidad alta en Google Chrome

CVE-2024-12053

High (8.8)

Impacto: Corrupción de objeto.

Resumen: Se ha detectado una vulnerabilidad en Google Chrome que permite a un atacante remoto explotar potencialmente la corrupción de objetos mediante una página HTML diseñada específicamente.

Versiones Afectadas

Versiones anteriores a la 131.0.6778.108/109 para Windows, Mac y Linux.
Ver +INFO.

Solución: Actualizar Google Chrome a la versión (131.0.6778.108/109 o posterior) desde la página oficial de actualizaciones de Chrome.
Ver +INFO.

Fecha de Publicación: 03/DIC/2024

SolarWinds Platform Cross-Site Scripting Vulnerability

CVE-2024-45717

High (7.0)

Impacto: Ejecución de comandos arbitrarios.

Resumen: Se ha detectado una vulnerabilidad en SolarWinds Platform que expone al software a ataques Cross-Site Scripting (XSS) en las secciones de búsqueda e información de nodos.

Versiones Afectadas

SolarWinds Platform Versión 2024.4 y anteriores.

Solución:

Actualizar los productos afectados a la última versión ofrecida por SolarWinds desde el sitio web oficial.
Ver +INFO.

Fecha de Publicación: 05/DIC/2024

Vulnerabilidad en IBM

CVE-2024-47115

High (7.8)

Impacto: Ejecución de comandos arbitrarios.

Resumen: Se ha descubierto una vulnerabilidad en IBM AIX que permite a un usuario local ejecutar comandos arbitrarios debido a una neutralización incorrecta de la entrada. Esta vulnerabilidad puede ser explotada por un atacante con privilegios locales para ejecutar comandos maliciosos en el sistema, lo que podría comprometer la seguridad.

Versiones Afectadas

- IBM AIX 7.2
- IBM AIX 7.3
- IBM VIOS 3.1
- IBM VIOS 4.1

Solución: Se recomienda aplicar las actualizaciones lo antes posible; para mayor detalle *Ver +INFO.*

Fecha de Publicación: 07/DIC/2024

Updates Available for Adobe FrameMaker

CVE-2024-53959

Adobe ha lanzado una actualización de seguridad para Adobe FrameMaker. Esta actualización aborda una vulnerabilidad crítica relacionada con una única Dynamic Link Library (DLL) en la plataforma Windows.

Recomendación:
Para remediar la vulnerabilidad, se recomienda aplicar las actualizaciones y parches de seguridad disponibles en la página oficial del fabricante. Para más detalles, consulte directamente el sitio web. *Ver +INFO*

Versiones Afectadas

- Adobe FrameMaker 2020 Release Update 7 and earlier
- Adobe FrameMaker 2022 Release Update 5 and earlier

Fecha de Publicación: 10/DIC/2024 +INFO

Actualizaciones de seguridad del mes de Diciembre para productos Microsoft

Las actualizaciones de seguridad de diciembre de 2024 de Microsoft corrigieron 74 vulnerabilidades en Windows, Office, SharePoint Server, Hyper-V, Defender para Endpoint y System Center Operations Manager. De estas, 2 se clasificaron como críticas, 51 como importantes y 21 como moderadas en términos de gravedad.

Recomendación:
Actualizar a la última versión disponible de los productos afectados desde la página web oficial del fabricante.

Versiones Afectadas

A continuación, algunos de los productos afectados:

- Windows Server
- Windows 10
- Windows 11

Para más información, consulte “+ *INFO*”

Fecha de Publicación: 16/DIC/2024 +INFO

LE PUEDE INTERESAR

Fecha De Publicación	Fabricante	CVE / Acceso	CVSSv3	Descripción
7/12/2024	IBM	CVE-2024-37071	5.3	Esta vulnerabilidad afecta a IBM Db2 para Linux, UNIX y Windows (incluido Db2 Connect Server) en las versiones 10.5, 11.1 y 11.5. Podría permitir a un usuario autenticado causar una denegación de servicio mediante una consulta especialmente diseñada, debido a una asignación incorrecta de memoria.
7/12/2024	IBM	CVE-2024-41762	5.3	Esta vulnerabilidad afecta a IBM Db2 para Linux, UNIX y Windows (incluido Db2 Connect Server) en las versiones 10.5, 11.1 y 11.5. Podría permitir a un atacante causar una denegación de servicio al hacer que el servidor se bloquee mediante una consulta especialmente diseñada.
7/12/2024	IBM	CVE-2024-47107	5.3	Esta vulnerabilidad afecta a IBM QRadar SIEM 7.5, permitiendo ataques de Cross-Site Scripting (XSS) almacenado. Los usuarios autenticados pueden inyectar código JavaScript arbitrario en la interfaz web, lo que podría alterar la funcionalidad y, potencialmente, exponer credenciales dentro de una sesión confiable.
7/12/2024	WordPress	CVE-2024-11464	6.1	El complemento Easy Code Snippets para WordPress es vulnerable a Cross-Site Scripting (XSS) reflejado debido a una insuficiente desinfección de la entrada y escape de salida en el parámetro 'page' en todas las versiones hasta la 1.0.2. Esto permite a atacantes no autenticados inyectar scripts maliciosos que se ejecutan si un usuario es engañado para hacer clic en un enlace.
9/12/2024	GoDaddy Email	CVE-2023-49156	4.3	Esta vulnerabilidad en GoDaddy Email Marketing permite la explotación de controles de acceso configurados incorrectamente, lo que podría llevar a una autorización faltante. Afecta a la versión 1.4.3 y anteriores de GoDaddy Email Marketing.

DESCUBIERTO NUEVO ROOTKIT SIGILOSO PARA LINUX: PUMAKIT

Pumakit es un malware avanzado para Linux que emplea técnicas avanzadas de sigilo y escalamiento de privilegios para operar de forma oculta en sistemas vulnerables. Descubierto por Elastic Security en un archivo llamado 'cron', su estructura incluye un dropper, módulos de kernel y espacio de usuario, y ejecutables en memoria. Aunque aún se desconocen sus objetivos, este tipo de malware suele dirigirse a infraestructuras críticas y sistemas empresariales.

Diseñado para kernels de Linux anteriores a la versión 5.7, Pumakit manipula el sistema mediante la función 'kallsyms_lookup_name()' y abusa de funciones del kernel para otorgar privilegios y ocultar actividad maliciosa. Su componente Kitsune SO refuerza estas capacidades, interceptando herramientas comunes y gestionando la comunicación con servidores de comando y control (C2).

El ATAQUE

El ataque comienza con un dropper llamado 'cron' que ejecuta cargas útiles en memoria. Estas manipulan la imagen del kernel para instalar el módulo rootkit ('puma.ko'), el cual utiliza técnicas avanzadas para escalar privilegios, alterar credenciales y ocultar su presencia. Kitsune SO complementa al rootkit del kernel, interceptando llamadas a nivel de usuario y ocultando archivos y procesos, mientras retransmite comandos e información al C2, asegurando el control completo del sistema comprometido. A continuación, se presentan los Indicadores de Compromiso (IoCs) que pueden ser incorporados en sus sistemas de seguridad.

INFO

CONTEXT	INDICATOR	(MD5)
ELF - ELF 64-bit LSB executable, x86-64, version 1 (SHA256)	cb070cc9223445113c3217f05ef85a930f626d3feaaea54d8585aaed3c2b3cfe	4375998ea157a8a21e1ead13052bad8a
ELF - ELF 64-bit LSB shared object, x86-64, version 1 (SHA256)	bbf0fd636195d51fb5f21596d406b92f9e3d05cd85f7cd663221d7d3da8af804	10913b57d02c52353b3217d1b371e661
ELF - ELF 64-bit LSB shared object, x86-64, version 1 (SHA256)	8ef63f9333104ab293eef5f34701669322f1c07c0e44973d688be39c94986e27	b21ae7ada5346dd59f582bba5b19bb31
ELF - ELF 64-bit LSB relocatable, x86-64, version 1 (SHA256)	8ad422f5f3d0409747ab1ac6a0919b1fa8d83c3da43564a685ae4044d0a0ea03	b5793af33aa19112ee45d56c51f268f7
ELF - ELF 64-bit LSB executable, x86-64, version 1 (SHA256)	71cc6a6547b5afda1844792ace7d5437d7e8d6db1ba995e1b2fb760699693f24	e9f0dca7acf31da96413f7f758b11272
IPv4	89.23.113.204	N/A
IPv4	89.23.113.20	N/A
HostName	rhel.opsecurity1.art	N/A
HostName	sec.opsecurity1.art	N/A

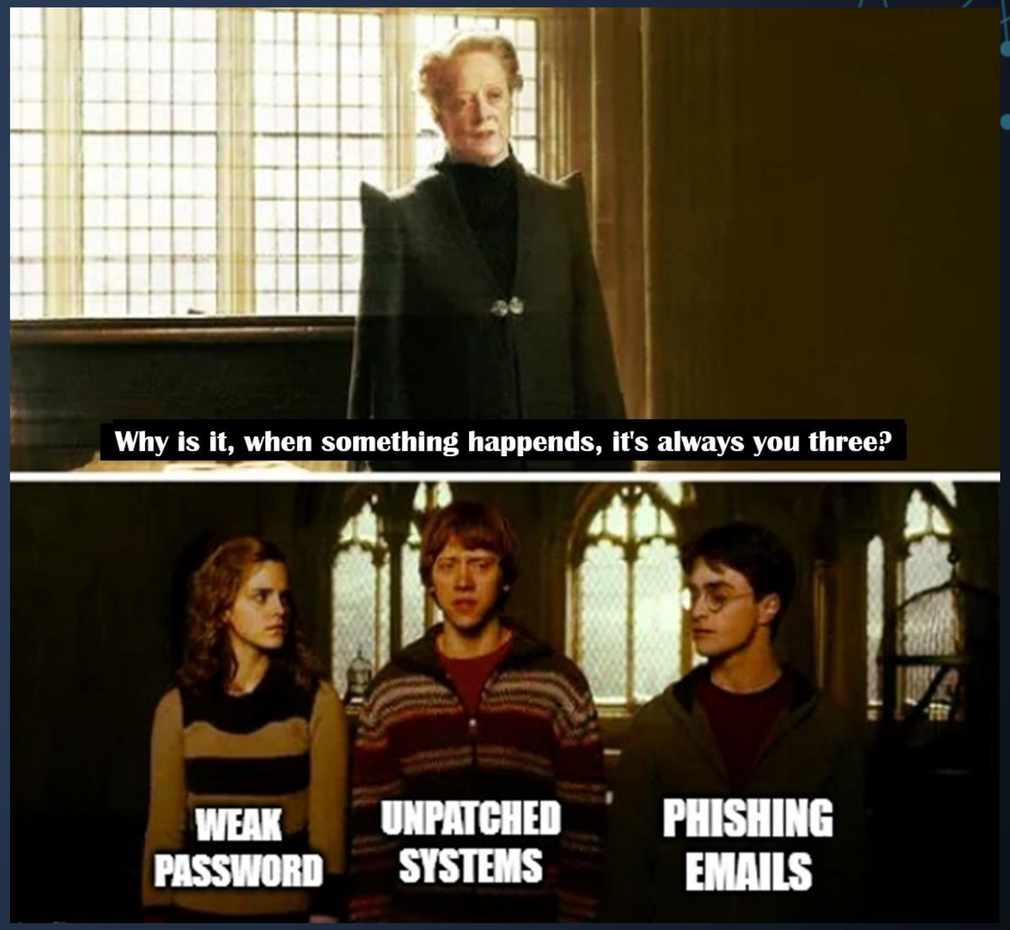
INFO

LOS TRES MOSQUETEROS DEL CAOS DIGITAL

Las amenazas de ciberseguridad suelen tener tres grandes culpables que, una y otra vez, protagonizan incidentes: contraseñas débiles, sistemas sin actualizar y correos de phishing. Estas vulnerabilidades son las puertas más comunes que los ciberdelincuentes utilizan para acceder a información confidencial, afectar la operatividad y comprometer la seguridad de las organizaciones.

Por ello, es fundamental adoptar medidas preventivas como el uso de contraseñas robustas y autenticación multifactor, mantener todos los sistemas y aplicaciones actualizados con los últimos parches de seguridad, y capacitar constantemente a los equipos para identificar y evitar intentos de phishing.

Fortalecer estas áreas críticas no solo reduce riesgos, sino que también asegura que la historia no se repita: la seguridad depende de todos y de las acciones que tomamos día a día.



DataSec

csirt_datasec@datasec.com.co

+57 310 285 8969