


Kit de Phishing 'Sneaky 2FA' basado en Telegram apunta a cuentas de Microsoft 365

TLP: CLEAR

31.01.2025





**CLICK PARA
EMPEZAR**



En esta edición:  [Telegram-Based "Sneaky 2FA" Phishing Kit Targets Microsoft 365 Accounts](#)

CONTENIDO



-  **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.



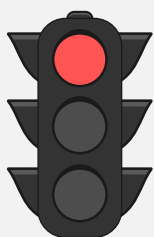
SOC

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 Meeting Management REST API Privilege Escalation Vulnerability

CVE-2025-20156



**Critical
(9.9)**

Impacto: Escalada de privilegios.

Resumen: Esta vulnerabilidad existe porque no se aplica la autorización adecuada a los usuarios de la API REST. Un atacante podría explotar esta vulnerabilidad enviando solicitudes API a un punto de acceso específico. Una explotación exitosa podría permitir al atacante obtener control a nivel de administrador sobre los nodos de borde gestionados por Cisco Meeting Management.

Versiones Afectadas

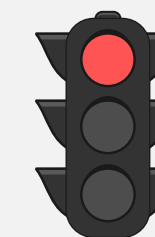
- Esta vulnerabilidad afecta a Cisco Meeting Management, sin importar la configuración del dispositivo.

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



Cisco BroadWorks SIP Denial of Service Vulnerability

CVE-2025-20165



**High
(7.5)**

Impacto: Denegación de servicios.

Resumen: Esta vulnerabilidad se debe a un manejo incorrecto de la memoria para ciertas solicitudes SIP. Un atacante podría explotar esta vulnerabilidad enviando una gran cantidad de solicitudes SIP a un sistema afectado. Un exploit exitoso podría permitir al atacante agotar la memoria asignada a los Servidores de Red de Cisco BroadWorks que gestionan el tráfico SIP.

Versiones Afectadas

- Esta vulnerabilidad afecta a Cisco BroadWorks, independientemente de la configuración del dispositivo.

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





IBM Analytics Content Hub is vulnerable to a buffer overflow

CVE-2024-39750



High (8.8)

Impacto: Ejecución código arbitrario.

Resumen: IBM Analytics Content Hub es vulnerable a varias fallas, incluyendo Buffer Overflow, Server Side Request Forgery (SSRF) y manejo incorrecto de errores, debido a componentes de código abierto. Un atacante podría explotar estas vulnerabilidades para ejecutar código arbitrario o afectar la estabilidad del sistema.

Versiones Afectadas

- IBM Analytics Content Hub 2.

Para más información, consulte [+ INFO](#).

Solución: Se recomienda aplicar las actualizaciones de seguridad mas recientes. Ver [+INFO](#)



SMA1000 Pre-Authentication Remote Command Execution Vulnerability

CVE-2025-23006



Critical (9.8)

Impacto: Ejecución de comandos arbitrarios.

Resumen: La vulnerabilidad de deserialización de datos no confiables previa a la autenticación en la consola de administración de dispositivos SMA 1000 (AMC) y la consola de administración central (CMC) podría permitir, en condiciones específicas, a un actor malicioso ejecutar comandos arbitrarios (RCE) del Sistema Operativo (SO) de forma remota y sin autenticarse.

Versiones Afectadas

- SonicWall SMA1000 Appliance Management Console (AMC) y Central Management Console (CMC) versión 12.4.3-02804 y versiones anteriores para plataformas Linux.

Solución: Se recomienda actualizar la ultima versiones disponibles desde el sitio oficial del fabricante. Ver [+INFO](#).





Vulnerabilidad en IBM Planning Analytics

CVE-2024-25034



**High
(8)**

Impacto: Carga de archivos ejecutables.

Resumen: IBM Planning Analytics podría ser vulnerable a la carga de archivos maliciosos debido a la falta de validación del tipo de archivo en el proceso File Manager T1. Los atacantes pueden aprovechar esta debilidad para cargar archivos ejecutables maliciosos en el sistema, que luego pueden ser enviados a las víctimas para realizar ataques adicionales.

Versiones Afectadas

- IBM Planning Analytics 2.0
 - IBM Planning Analytics 2.1
- Para más información, consulte [+INFO](#).

Solución: Se recomienda aplicar las actualizaciones de seguridad mas recientes. Ver [+INFO](#)



IBM Sterling B2B Integrator is Vulnerable to Remote Code Execution

CVE-2024-31903



**High
(8.8)**

Impacto: Ejecución de código arbitrario.

Resumen: IBM Sterling B2B Integrator Standard Edition permite que un atacante en la red local ejecute código arbitrario en el sistema, debido a la deserialización de datos no confiables.

Versiones Afectadas

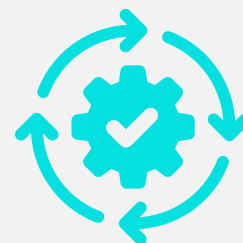
- IBM Sterling B2B Integrator 6.2.0.0 - 6.2.0.2
- IBM Sterling B2B Integrator 6.0.0.0 - 6.1.2.5.

Solución: Se recomienda aplicar las actualizaciones de seguridad mas recientes. Ver [+INFO](#)



Actualización de Seguridad para GitLab CE/EE

CVE-2025-0314; CVE-2024-1193; CVE-2024-6324



Git lab ha lanzado actualizaciones de seguridad que abordan tres vulnerabilidades, incluida una de gravedad “alta” y dos de gravedad “media” que afectan a GitLab Community Edition (CE) y Enterprise Edition (EE)

Recomendación:

Actualizar el producto para a la última versión disponible que resuelven las vulnerabilidades encontradas.

Versiones Afectadas

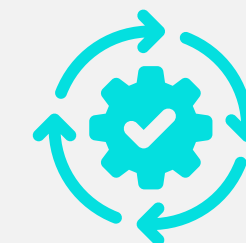
- 17.2.x y anteriores a 17.6.4
- 17.7.x y versiones anteriores a 17.7.3
- 17.8.x y versiones anteriores a 17.8.1

Ver +INFO.



Oracle Releases January 2025 Patch to Address 318 Flaws Across Major Products

CVE-2025-21556, CVE-2024-21287, CVE-2025-21524, CVE-2023-3961, CVE-2024-23807, CVE-2023-46604



Oracle ha lanzado una actualización de parches para corregir 318 vulnerabilidades en varios de sus productos y servicios, incluyendo Oracle Agile PLM Framework, JD Edwards EnterpriseOne Tools, Oracle WebLogic Server, y Oracle Communications. Se recomienda a los usuarios aplicar estos parches para proteger sus sistemas. Además, se han lanzado 285 parches de seguridad para Oracle Linux.

Recomendación:

Se recomienda a los usuarios de productos Oracle aplicar la actualización crítica de parches de enero de 2025 para corregir vulnerabilidades de seguridad y proteger sus sistemas contra posibles explotaciones. Ver +INFO

Versiones Afectadas

A continuación, se presenta algunas de las vulnerabilidades:

- MySQL Cluster,
- Oracle Hyperion,
- Oracle Communications

Para más información Ver +INFO.

LE PUEDE INTERESAR

FECHA DE PUBLICACIÓN	FABRICANTE	CVE / ACCESO	CVSSV3	DESCRIPCIÓN
22/01/2025	Cisco	CVE-2025-20128	5.3	Esta vulnerabilidad se debe a un desbordamiento de enteros en una comprobación de límites que permite una lectura de desbordamiento de búfer en el heap. Un atacante podría explotar esta vulnerabilidad enviando un archivo manipulado que contenga contenido OLE2 para que sea escaneado por ClamAV en un dispositivo afectado.
25/01/2025	IBM	CVE-2023-38713	5.3	IBM Cloud Pak System iFix1 podrían revelar información sensible sobre el sistema, lo que podría facilitar futuros ataques contra el mismo.
25/01/2025	IBM	CVE-2023-38271	4.3	IBM Cloud Pak System iFix1 podrían permitir que un usuario autenticado obtenga información sensible de los archivos de registro.
25/01/2025	IBM	CVE-2024-35134	5.3	IBM Analytics Content Hub 2.0 podría permitir que un atacante remoto obtenga información sensible cuando un mensaje de error técnico detallado se devuelve en el navegador. Esta información podría ser utilizada en futuros ataques contra el sistema.
25/01/2025	IBM	CVE-2024-35113	4.3	IBM Control Center 6.2.1 y 6.3.1 podrían permitir que un usuario autenticado obtenga información sensible expuesta a través de un listado de directorios.
25/01/2025	IBM	CVE-2024-35144	5.3	IBM Maximo Application Suite 8.10, 8.11 y 9.0 - El componente Monitor almacena código fuente en el servidor web, lo que podría facilitar futuros ataques contra el sistema.
25/01/2025	IBM	CVE-2024-35150	5.3	IBM Maximo Application Suite 8.10.12, 8.11.0, 9.0.1 y 9.1.0 - El componente Monitor no neutraliza la salida escrita en los registros, lo que podría permitir a un atacante inyectar entradas falsas en los registros.
25/01/2026	IBM	CVE-2024-35148	6.3	IBM Maximo Application Suite 8.10.10, 8.11.7 y 9.0 - El componente Monitor es vulnerable a inyecciones SQL. Un atacante remoto podría enviar declaraciones SQL especialmente diseñadas, lo que le permitiría ver, agregar, modificar o eliminar información en el sistema de back-end
25/01/2027	IBM	CVE-2024-35145	6.1	IBM Maximo Application Suite 9.0.0 - El componente Monitor es vulnerable a ataques de cross-site scripting (XSS). Esta vulnerabilidad permite a un atacante no autenticado insertar código JavaScript arbitrario en la interfaz web, lo que altera la funcionalidad prevista y podría conducir a la divulgación de credenciales dentro de una sesión confiable.
25/01/2028	WordPress	CVE-2025-0357	9.8	El plugin WPBookit para WordPress es vulnerable a cargas de archivos arbitrarios debido a una validación insuficiente del tipo de archivo en la función 'WPB_Profile_controller::handle_image_upload' en versiones hasta, e incluyendo, la 1.6.9. Esto permite a atacantes no autenticados cargar archivos arbitrarios en el servidor del sitio afectado, lo que podría hacer posible la ejecución remota de código.



Kit de Phishing 'Sneaky 2FA' Basado en Telegram Apunta a Cuentas de Microsoft 365

En diciembre de 2024, Sekoia.io descubrió un nuevo kit de phishing dirigido a cuentas de Microsoft 365, llamado Sneaky 2FA. Este kit se ofrece como un servicio de Phishing-as-a-Service (PhaaS) a través de un bot en Telegram, permitiendo a los ciberdelincuentes implementar páginas de phishing personalizadas. Sneaky 2FA emplea técnicas avanzadas de evasión, como la obfuscación de código y la integración con Cloudflare Turnstile, lo que dificulta su detección. Los atacantes pueden usar infraestructura comprometida, como sitios WordPress, para alojar las páginas de phishing. El kit también pre-rellena automáticamente las direcciones de correo electrónico de las víctimas y utiliza patrones de URL complejos para evitar la detección. Además, los pagos por el servicio se realizan mediante criptomonedas, lo que sugiere actividades de lavado de dinero. Para mitigar los riesgos, se recomienda implementar métodos de autenticación resistentes a phishing (como FIDO2/WebAuthn), realizar análisis en tiempo real de las URLs y monitorear registros de autenticación en busca de anomalías.

EL ATAQUE

Sneaky 2FA es un kit de phishing dirigido a cuentas de Microsoft 365, disponible como un servicio en Telegram. Permite a los atacantes crear páginas de phishing personalizadas para robar credenciales y cookies de sesión. Utiliza técnicas de evasión como la ofuscación de código, pre-relleno de correos electrónicos y anti-bot con Cloudflare Turnstile. Los pagos se realizan mediante criptomonedas, lo que sugiere actividades de lavado de dinero.



CONTEXT	INDICATOR	(MD5)
URL	[highnationservices.][com/n/%23victim]@[example.com]	N/A
HTML document text	205f791806ee1580b37807b1a6be0279349760151adc81d3791f32b5d4c2e9ea	8c1936dffed7963a948b55b2b818796c
MS Windows icon resource	5d91563b6acd54468ae282083cf9ee3d2c9b2daa45a8de9cb661c2195b9f6cbf	7cdd5a7e87e82d145e7f82358f9ebd04
IPV4	101.99.92.124	N/A
IPV4	185.125.100.81	N/A
URL	[128.0].[0.0]	N/A
URL	[129.0].[0.0]	N/A
empty	E3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	d41d8cd98f00b204e9800998ecf8427e
URL	[185.125].[100.81/api/key]	N/A
URL	[mysilverfox.][com.my/][00/%23victim]@[example.com]	N/A
URI	[sneakylog.][store/api/key]	N/A
URL	[Africanagrirmarket][.com]	N/A



+ INFO



¡Importancia de la Verificación de Correos y Datos para la Seguridad Digital!

La verificación de correos electrónicos y la comprobación de datos antes de actuar son prácticas esenciales para garantizar la seguridad en los entornos digitales. Dado el aumento de fraudes, estafas y ciberataques, es crucial validar la autenticidad de los correos recibidos. Muchos intentan suplantar entidades legítimas, como bancos, para obtener información sensible o acceder a sistemas privados. Antes de hacer clic en enlaces o descargar archivos adjuntos, se debe comprobar si el remitente es confiable, revisar la dirección de correo y buscar posibles errores ortográficos o tonos sospechosos. Además, es recomendable implementar herramientas de protección de correo electrónico, como filtros avanzados contra spam, sistemas de autenticación de correos, y tecnologías que detecten y bloqueen correos fraudulentos, garantizando así una mayor seguridad en las comunicaciones..

Yo: Ya instale el programa de que nos pidieron los de sistemas

Sistemas: No hemos pedido nada...

Yo: ¿Y el correo que llegó hoy?

Sistemas:





 csirt_datasec@datasec.com.co

 +57 310 285 8969

