

**BOLETÍN CIBERSEGURIDAD
CSIRT - DATASEC**



DataSec



RANSOMWARE BIANLIAN AHORA SE CENTRA EN EL ROBO DE DATOS.

TLP: CLEAR

02.12.2024

**CLICK PARA
EMPEZAR**







En esta edición: →

Nuevas tácticas usadas por el Ransomware BianLian

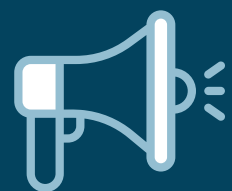
CONTENIDO



-  **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 Secure Web Appliance Privilege Escalation Vulnerability

CVE-2024-20435



High
(8.8)

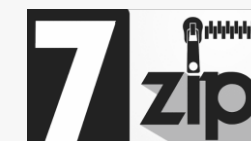
Impacto: Escalada de privilegios.

Resumen: Esta vulnerabilidad se debe a una validación insuficiente de la entrada proporcionada por el usuario para la CLI. Un atacante podría explotar esta vulnerabilidad autenticándose en el sistema y ejecutando un comando manipulado en el dispositivo afectado.

Versiones Afectadas

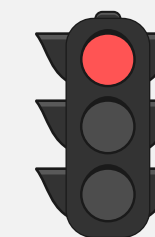
Esta vulnerabilidad afecta a Cisco AsyncOS para Secure Web Appliance, tanto en dispositivos virtuales como físicos.

Solución: Cisco ha publicado actualizaciones de software que solucionan esta vulnerabilidad. [Ver +INFO](#)



7-Zip Zstandard Decompression Integer Underflow Remote Code Execution Vulnerability

CVE-2024-11477



High
(7.8)

Impacto: Inyección de comandos.

Resumen: Se ha identificado una vulnerabilidad de tipo 'integer underflow' causada por una validación inadecuada de datos en la implementación del componente de manejo de descompresión Zstandard. Esta falla podría permitir que un actor malicioso remoto ejecute código arbitrario.

Versiones Afectadas

7-Zip – Versiones anteriores a 24.07

Solución: Actualizar los productos afectados a la última versión disponible desde la página web. [Ver +INFO](#).



Authentication Bypass in the Management Web Interface

CVE-2024-0012



Critical
(9.3)

Impacto: Escalada de privilegios.

Resumen: Una vulnerabilidad en PAN-OS de Palo Alto Networks permite a atacantes no autenticados acceder a la interfaz web de administración y obtener privilegios de administrador, posibilitando acciones administrativas y la explotación de otras vulnerabilidades.

Versiones Afectadas

Algunas de las versiones afectadas a continuación:

- PAN-OS 11.2
- PAN-OS 11.1

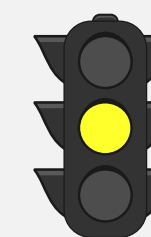
Ver [+INFO](#) para ver el detalle de las versiones afectadas

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](#)



Firewall Denial of Service (DoS) in GlobalProtect Gateway Using a Specially Crafted Packet

CVE-2024-2550



Medium
(6.6)

Impacto: Denegación de servicios.

Resumen: La vulnerabilidad permitiría a un atacante no autenticado detener el servicio GlobalProtect del Firewall al enviar un paquete malicioso causando una condición tipo Denial of Service (DoS).

Versiones Afectadas

Algunas de las versiones afectadas a continuación:

- PAN-OS 11.2
- PAN-OS 11.1

Ver [+INFO](#) para ver el detalle de las versiones afectadas

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](#)



Vulnerabilidad en Google Chrome

CVE-2024-11395



High
(8.8)

Impacto: Ejecución de código.

Resumen: Type Confusion en V8 de Google Chrome, en versiones anteriores a la 131.0.6778.85, permitió que un atacante remoto pudiera explotar potencialmente una "heap corruption" mediante una página HTML especialmente diseñada.

Versiones Afectadas

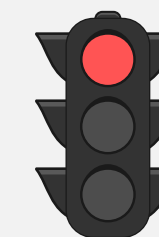
- Windows, Mac: versiones anteriores a la 131.0.6778.85/.86.
- Linux: versiones anteriores a la 131.0.6778.85.

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



Oracle Security Alert Advisory

CVE-2024-21287



High
(7.5)

Impacto: Acceso no autorizado.

Resumen: Una vulnerabilidad en Oracle Agile PLM Framework permite a atacantes no autenticados comprometer el sistema a través de HTTP, lo que podría dar acceso no autorizado a datos críticos o a toda la información del entorno.

Versiones Afectadas

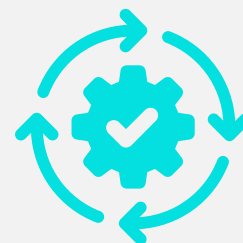
- Oracle Agile PLM Framework, version 9.3.6.

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



VMware Aria Operations updates address multiple vulnerabilities

CVE-2024-38830, CVE-2024-38831, CVE-2024-38832, CVE-2024-38833, CVE-2024-38834



Se han reportado de manera responsable múltiples vulnerabilidades en VMware Aria Operations a VMware. Ya están disponibles actualizaciones para remediar estas vulnerabilidades en el producto afectado.

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.

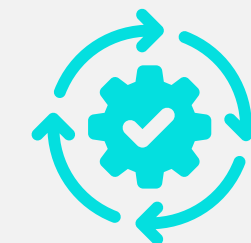
[Ver +INFO](#)

Versiones Afectadas

- VMware Aria Operations



Actualizaciones de seguridad del mes de noviembre para productos Microsoft



Microsoft ha lanzado actualizaciones de seguridad para múltiples productos. Estas actualizaciones resuelven 89 vulnerabilidades, incluidas 4 vulnerabilidades de tipo zero-day.

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:

- NET and Visual Studio
- Airlift.microsoft.com
- Microsoft Graphics Component

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

LE PUEDE INTERESAR

FECHA DE PUBLICACIÓN	FABRICANTE	CVE / ACCESO	CVSSV3	DESCRIPCIÓN
15/11/2024	Apache	CVE-2024-45784	7.5	Esta vulnerabilidad permite a los autores de DAGs registrar, de manera no intencional o intencional, variables de configuración sensibles. Los usuarios no autorizados podrían acceder a estos registros, lo que podría exponer datos críticos que podrían ser utilizados para comprometer la seguridad de la implementación de Airflow.
15/11/2024	Fortinet	CVE-2024-26011	5.2	Una vulnerabilidad de autenticación incorrecta [CWE-287] en el demonio fgfmd de FortiManager, FortiOS, FortiPAM, FortiPortal, FortiProxy y FortiSwitchManager podría permitir a un atacante no autenticado inyectar (pero no recibir) paquetes en los túneles establecidos entre un FortiManager y el dispositivo objetivo.
15/11/2024	Fortinet	CVE-2024-33505	5.3	Una vulnerabilidad de desbordamiento de búfer basado en heap [CWE-122] en el demonio httpd de FortiManager y FortiAnalyzer podría permitir a un atacante remoto no autenticado ejecutar código o comandos arbitrarios como un usuario de baja privilegio a través de solicitudes especialmente diseñadas.
18/11/2024	PostgreSQL	CVE-2024-10979 CVE-2024-10976 CVE-2024-10978 CVE-2024-10977	8.8 4.2 4.2 3.1	Se han detectado 4 vulnerabilidades en el sistema de gestión de base de datos PostgreSQL, incluyendo una vulnerabilidad de severidad alta. Estas vulnerabilidades permitirían la ejecución de código arbitrario.
19/11/2024	IBM	CVE-2024-37070	4.3	IBM Concert Software 1.0.0, 1.0.1, 1.0.2 y 1.0.2.1 podría permitir que un usuario autenticado obtenga información confidencial que podría contribuir a futuros ataques contra el sistema.
19/11/2024	IBM	CVE-2024-52359	4.3	IBM Concert Software 1.0.0, 1.0.1, 1.0.2 y 1.0.2.1 podría permitir que un usuario autenticado realice acciones no autorizadas que deberían estar reservadas al administrador debido a controles de acceso inadecuados.
19/11/2024	IBM	CVE-2024-52360	7.6	IBM Concert Software 1.0.0, 1.0.1, 1.0.2 y 1.0.2.1 es vulnerable a la inyección SQL. Un atacante remoto podría enviar instrucciones SQL especialmente manipuladas, que podrían permitirle ver, agregar, modificar o eliminar información en la base de datos back-end.
20/11/2024	WordPress	CVE-2024-10515	3.5	En el proceso de prueba del complemento SEO de WordPress de Squirrly SEO Plugin anterior a la versión 12.3.21, se encontró una vulnerabilidad que permite implementar XSS almacenado en nombre del editor mediante la incorporación de un script malicioso, lo que implica una puerta trasera de apropiación de cuentas.
20/11/2024	WordPress	CVE-2024-10913	8.8	El complemento Clone para WordPress es vulnerable a la inyección de objetos PHP en todas las versiones hasta la 2.4.6 incluida, a través de la deserialización de entradas no confiables en la función 'recursive_unserialized_replace'. Esto hace posible que atacantes no autenticados inyecten un objeto PHP. No existe ninguna cadena POP conocida en el software vulnerable. Si existe una cadena POP a través de un complemento o tema adicional instalado en el sistema de destino, podría permitir al atacante eliminar archivos arbitrarios, recuperar datos confidenciales o ejecutar código.



CISA INFORMA QUE EL RANSOMWARE BIANLIAN AHORA SE CENTRA EXCLUSIVAMENTE EN EL ROBO DE DATOS.

El grupo de ransomware BianLian ha cambiado su enfoque y ahora opera principalmente como un grupo de extorsión basado en el robo de datos, dejando de lado el cifrado de sistemas. Desde enero de 2024, se concentra exclusivamente en exfiltrar datos para extorsionar, utilizando herramientas como credenciales de Remote Desktop Protocol (RDP) robadas, backdoors personalizados y modificaciones en el registro de Windows. Este cambio de tácticas refleja su adaptación a un modelo más dirigido y sofisticado.

BianLian ha listado 154 víctimas en su portal de extorsión, que incluyen tanto pequeñas y medianas empresas e inclusive grandes organizaciones. Aunque han reclamado ataques recientes a empresas globales, algunos de estos casos aún no han sido confirmados. Su evolución estratégica subraya la importancia de implementar medidas de seguridad robustas para mitigar amenazas como estas.

EL ATAQUE

El aviso actualizado describe nuevas tácticas del grupo de atacantes, que incluyen la explotación de la cadena de vulnerabilidades ProxyShell (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207) para comprometer infraestructuras Windows y ESXi, y el uso de herramientas como Ngrok y Rsocks para enmascarar destinos mediante túneles SOCKS5. Además, explotan la vulnerabilidad CVE-2022-37969 para escalar privilegios en Windows 10 y 11. Para evadir detección, emplean empaquetado UPX y renombrado de binarios con nombres legítimos de servicios. También crean cuentas Domain Admin y Azure AD, colocan webshells en servidores Exchange y utilizan PowerShell para comprimir datos antes de su exfiltración. El grupo ha comenzado a incluir un Tox ID en las notas de rescate y emplea tácticas de presión, como imprimir notas en impresoras conectadas a la red y realizar llamadas telefónicas a empleados de las víctimas.



CONTEXT	INDICATOR	MD5
(SHA256) PEXE - PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS Windows	1fd07b8d1728e416f897bef4f1471126f9b18ef108eb952f4b75050da22e8e43	08e76dd242e64bb31aec09db8464b28f
(SHA256) PEXE - PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS Windows	7b15f570a23a5c5ce8ff942da60834a9d0549ea3ea9f34f900a09331325df893	ad5fbd52096e8bdc76d4052a5d8975a2
(SHA256) PEXE - PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows	40126ae71b857dd22db39611c25d3d5dd0e60316b72830e930fba9baf23973ce	e245f8d129e8eadb00e165c569a14b71
URL	http://bianlianlbc5an4kgnay3opdemgcryg2kpfcbgczopmm3dnbz3uaunad.onion	N/A
URL	http://bianlivemqbawcco4cx4a672k2fip3guyxudzurfqvdszafam3ofggqd.onion	N/A
Domain	gnay3opdemgcryg2kpfcbgczopmm3dnbz3uaunad.onion	N/A
Email	n0torious@onionmail.org	N/A
Email	swikipedia@onionmail.org	N/A
Email	xwikipedia@onionmail.org	N/A
URL	http://94.158.244.69:443	N/A

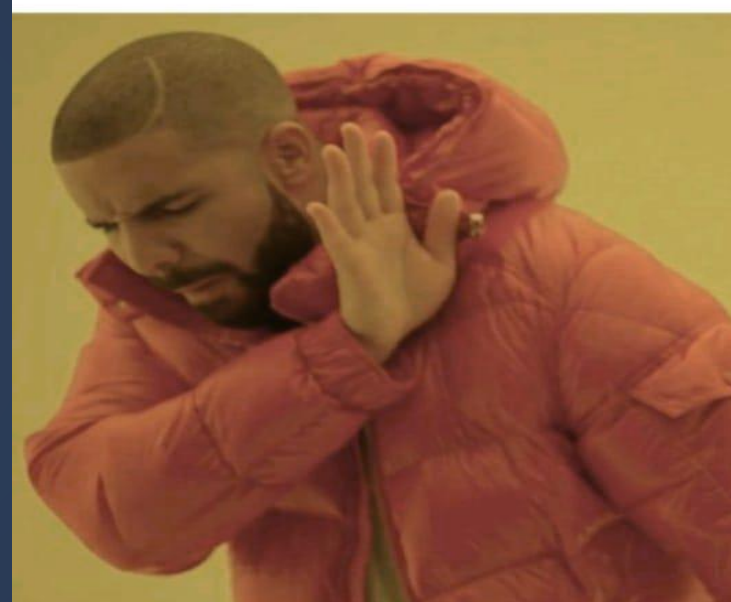


+ INFO



Del cifrado al chantaje: La evolución del ransomware

Los ataques de ransomware han evolucionado y ahora, en lugar de centrarse únicamente en cifrar archivos, los atacantes optan por robar información confidencial para extorsionar a las víctimas bajo la amenaza de divulgar los datos comprometidos. Este enfoque ha incrementado el impacto potencial al afectar tanto la operatividad como la reputación de las organizaciones. Por ello, es esencial reforzar las defensas mediante soluciones de seguridad avanzadas, respaldos frecuentes y políticas estrictas de acceso a la información sensible, además de contar con un plan de respuesta ante incidentes para detectar y mitigar rápidamente cualquier amenaza.



When CISO asks for \$1M for proactive cybersecurity




When hacker asks for \$10M ransomware



DataSec

 csirt_datasec@datasec.com.co

 +57 310 285 8969



© 2024 DataSec SAS. Todos los Derechos Reservados