
# BOLETÍN DE CIBERSEGURIDAD

## ABRIL 2023

ADV

# ÍNDICE


NOTICIAS INTERNACIONALES 3

Quadreams acusada de emplear spyware contra figuras políticas y periodistas 4

Boletín de seguridad de Android de abril 5

PoC de malware polimórfico empleando Inteligencia Artificial 6

Descubierto un error de diseño en Azure que permite tomar el control de cuentas 7

Encontradas muestras de LockBit dirigidas contra sistemas macOS Identificada nueva campaña de QBot, 8

Vulnerabilidades críticas en las bases de datos PostgreSQL de Alibaba Cloud 9

NOTICIAS NACIONALES 10

Comisión de Seguridad de la Información en México, aún sin Ley de Ciberseguridad 11

VULNERAVILIDADES RELEVANTES 12

Tabla de vulnerabilidades relevantes: Abril 2023 13

Fabricantes y sus vulnerabilidades relevantes: Abril 2023 15

Empresas Multinacionales y sus vulnerabilidades: Abril 2023 16

CULTURA DE CIBERSEGURIDAD 17

Troyano 18

REFERENCIAS 21

# NOTICIAS INTERNACIONALES

# QUADREAMS ACUSADA DE EMPLEAR SPYWARE CONTRA FIGURAS POLÍTICAS Y PERIODISTAS

INVESTIGADORES DE CITIZENLAB JUNTO AL EQUIPO DE THREAT INTELLIGENCE DE MICROSOFT HAN PUBLICADO UNA INVESTIGACIÓN ACERCA DE LA COMPAÑÍA ISRAELÍ QUADREAMS


Marczak, B. (2023, April 11). Sweet QuaDreams: A First Look at Spyware Vendor QuaDream's Exploits, Victims, and Customers - The Citizen Lab. The Citizen Lab. https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/

Quien acusan de emplear spyware contra periodistas y figuras políticas.

La actividad de la empresa de basaría en la venta y distribución de una plataforma denominada Reign a entidades gubernamentales, a la que Microsoft describe como un conjunto de exploits, malware e infraestructura diseñado para exfiltrar información de dispositivos móviles.

De las técnicas empleadas para su funcionamiento destaca lo que los investigadores sospechan que es un exploit zero-click para dispositivos iOS, al que han denominado ENDOFDAYS, que haría uso de invitaciones invisibles de iCloud.

El análisis habría identificado al menos cinco víctimas, que por ahora continúan siendo anónimas, en Norteamérica, Asia central, el Sudeste Asiático, Europa y Oriente Medio.

# BOLETÍN DE SEGURIDAD DE ANDROID DE ABRIL

EL BOLETÍN DE SEGURIDAD DE ANDROID CONTIENE DETALLES DE LAS VULNERABILIDADES DE SEGURIDAD QUE AFECTAN A LOS DISPOSITIVOS ANDROID.

Boletín de seguridad de Android: abril de 2023. (2023). Android Open Source Project. https://source.android.com/docs/security/bulletin/2023-04-01?hl=es-41

Los niveles de parches de seguridad de 2023-04-05 o posteriores abordan todos estos problemas. Para obtener información sobre cómo verificar el nivel del parche de seguridad de un dispositivo, consulte Verifique y actualice su versión de Android .

Los socios de Android son notificados de todos los problemas al menos un mes antes de la publicación. Los parches de código fuente para estos problemas se publicaron en el repositorio del Proyecto de código abierto de Android (AOSP) y se vincularon desde este boletín. Este boletín también incluye enlaces a parches fuera de AOSP.

# DESCUBIERTO UN ERROR DE DISEÑO EN AZURE QUE PERMITE TOMAR EL CONTROL DE CUENTAS

UNA INVESTIGACIÓN DE ORCA HA DEMOSTRADO LA EXISTENCIA DE UN ERROR DE DISEÑO EN MICROSOFT AZURE SHARED KEY


Nisimi, R. (2023). From listKeys to Glory: How We Achieved a Subscription Privilege Escalation and RCE by Abusing Azure Storage Account Keys. Complete Cloud Security in Minutes - Orca Security. https://orca.security/resources/blog/azure-shared-key-authorization-exploitation/

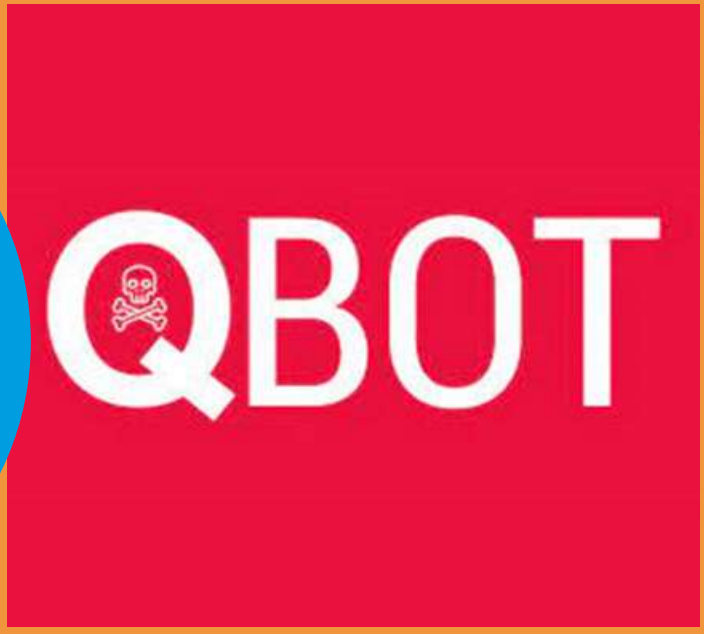
Que permitiría a un atacante obtener acceso a las cuentas de almacenamiento de Microsoft Storage.

Aunque Orca ha publicado una prueba de concepto en la que demuestra cómo se puede robar tokens de acceso de identidades con privilegios más altos, moverse lateralmente, acceder a activos comerciales críticos y ejecutar código remoto (RCE), el Security Response Center de Microsoft ha considerado el problema como un fallo de diseño y no una vulnerabilidad, por lo que no puede ofrecer una actualización de seguridad y habrá que esperar a un rediseño de Azure.

Mientras tanto, se recomienda eliminar la autorización de clave compartida de Azure y, en su lugar, adoptar la autenticación de Azure Active Directory como estrategia de mitigación.

# ENCONTRADAS MUESTRAS DE LOCKBIT DIRIGIDAS CONTRA SISTEMAS MACOS IDENTIFICADA NUEVA CAMPAÑA DE QBOT,

MALWAREHUNTERTEAM HA ENCONTRADO UNA MUESTRA DE UN ARCHIVO DE LOCKBIT QUE CONTIENE LA CAPACIDAD DE INFECTAR NUMEROSOS SISTEMAS OPERATIVOS, INCLUYENDO POR PRIMERA VEZ, MACOS DE APPLE.




Tech, T. (2023, April 21). Boletín semanal de Ciberseguridad, 15 – 21 de abril - Think Big Empresas. Think Big. https://empresas.blogthinkbig.com/boletin-semanal-de-ciberseguridad-15-21-abril-2023/

MalwareHunterTeam resalta que se trata de un hito remarcable pues también es la primera vez que se tiene conocimiento de uno de los grandes grupos de ransomware creando un malware dirigido específicamente a macOS.

El archivo encontrado incluye un cifrador llamado 'locker_Apple_M1_64', para los dispositivos de Apple más recientes y otro para PowerPC CPUs, usado por los macOS más antiguos.

Un análisis en profundidad del archivo muestra que, por el momento, se trata de una versión inicial de esta cepa de LockBit y que no podría usarse en un ataque real, pero muestra el interés de este ransomware en atacar dispositivos macOS en un futuro próximo.

# NUEVA POC PERMITE REALIZAR BYPASS EN VM2 SANDBOX

INVESTIGADORES DE SEGURIDAD HAN PUBLICADO UNA NUEVA POC CAPAZ DE REALIZAR BYPASS EN VM2 SANDBOX,

Boletín de seguridad de Android: abril de 2023. (2023b). Android Open Source Project. https://source.android.com/docs/security/bulletin/2023-04-01?hl=es-419

Ampliamente utilizada en el mundo del desarrollo y la seguridad para ejecutar y probar código que no es de confianza en un entorno aislado.

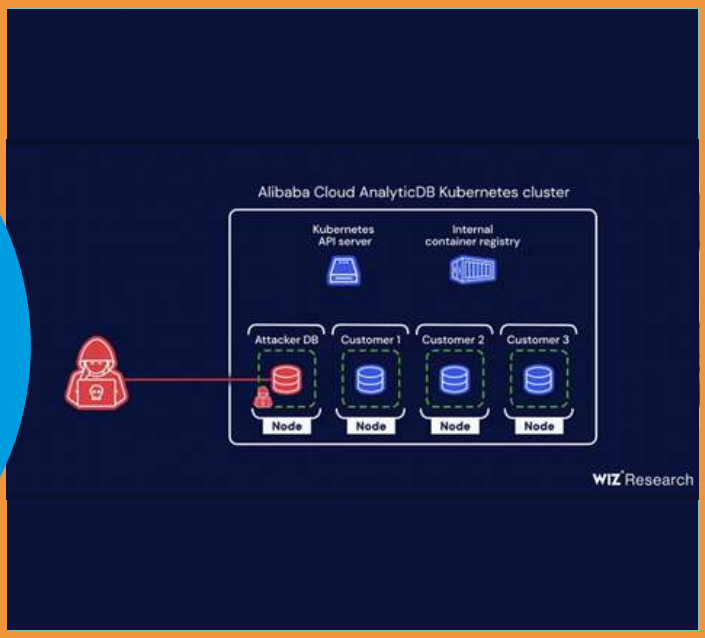
Este bypass permitiría ejecutar malware fuera de las limitaciones del entorno sandbox. La primera vulnerabilidad fue identificada como CVE-2023-29017 hace dos semanas, y las dos últimas identificadas como CVE-2023-29199 y CVE-2023-30547.

Esta última vulnerabilidad, con un CVSS de 9.8, puede ser aprovechada por actores maliciosos debido a un fallo de sanitización que permite al atacante lanzar una excepción de host dentro de “handleException()”.

Se recomienda a los usuarios que para corregir la vulnerabilidad actualicen a la versión 3.9.17 lo antes posible para evitar un posible incidente de seguridad.

# VULNERABILIDADES CRÍTICAS EN LAS BASES DE DATOS POSTGRESQL DE ALIBABA CLOUD

WIZ RESEARCH HA DESCUBIERTO UNA CADENA DE VULNERABILIDADES CRÍTICAS EN DOS DE LOS SERVICIOS POPULARES DE ALIBABA CLOUD, APSARADB RDS PARA POSTGRESQL Y ANALYTICDB PARA POSTGRESQL.




#BrokenSesame: Accidental 'write' permissions to private registry allowed potential RCE to Alibaba Cloud Database Services | Wiz Blog. (2023, April 27). wiz.io. https://www.wiz.io/blog/brokensesame-accidental-write-permissions-to-private-registry-allowed-potential-r

Apodadas #BrokenSesame, las vulnerabilidades permitieron potencialmente el acceso no autorizado a las bases de datos PostgreSQL de los clientes de Alibaba Cloud y la capacidad de realizar un ataque a la cadena de suministro en ambos servicios de bases de datos de Alibaba, lo que llevó a un RCE en los servicios de bases de datos de Alibaba .

Esta investigación demuestra dos riesgos críticos que todo equipo de seguridad debe tener en cuenta:

El riesgo de un aislamiento inadecuado en aplicaciones multiinquilino: al aprovechar algunos comportamientos inseguros a nivel de contenedor, pudimos escapar al nodo K8s y obtener altos privilegios dentro del clúster K8s. .

Esto, a su vez, nos permitió acceder a las bases de datos de otros inquilinos, lo que podría comprometer a todos los usuarios de un servicio

El riesgo de permisos de escritura con alcance inadecuado para registros de contenedores: una vez que comprometimos el nodo K8s, examinamos los permisos de las credenciales configuradas que se usan para extraer imágenes del registro de contenedores privados de Alibaba Cloud.

Debido a una mala configuración crítica, las credenciales también tenían permisos de escritura en el registro. Esto significaba que teníamos la capacidad de sobrescribir imágenes de contenedores en el registro central de imágenes utilizado por Alibaba Cloud y potencialmente llevar a cabo un ataque a la cadena de suministro a gran escala en los servicios de base de datos de Alibaba Cloud.

# NOTICIAS NACIONALES

# COMISIÓN DE SEGURIDAD DE LA INFORMACIÓN EN MÉXICO, AÚN SIN LEY DE CIBERSEGURIDAD

ACTUALMENTE, MÉXICO NO CUENTA CON UNA LEGISLACIÓN EN MATERIA DE CIBERSEGURIDAD, LO QUE TIENE COMO CONSECUENCIA QUE MÚLTIPLES INSTITUCIONES GUBERNAMENTALES, ASÍ COMO EMPRESAS PRIVADAS Y PERSONAS NATURALES, SEAN VÍCTIMAS DE CIBERATAQUES.

Murillo, F. (2023, April 28). México aún no cuenta con legislación ante ciberataques: Delta Protect. Grupo Milenio. https://www.milenio.com/negocios/delta-protect-mexico-no-cuenta-con-legislacion-de-ciberataques

Esto a pesar de que desde 2018 se propusieron 11 iniciativas de leyes sobre este tema.

Durante su participación en el foro Ciberseguridad y cumplimiento: Lo que toda startup debe saber, organizado por Delta Protect y BBVA Spark, Juan Carlos Carrillo destacó que las regulaciones en el país respecto a asuntos de ciberseguridad y privacidad de la información, en muchos casos, no tienen el mismo nivel de madurez que otros países o regiones.

Ante ese panorama se esperaba que la nueva Ley Federal de Ciberseguridad se publicara el pasado diciembre, sin embargo, “hasta la fecha, no está disponible para ser descargada por el público general”, dijo Santiago Fuentes Rivera, co-fundador y director general de Delta Protect.

¿Cómo se protegen las empresas mexicanas de los hackeos?

En el país la ciberseguridad en las empresas se fortaleció después de la pandemia, ante los años de constante disrupción, aumento de la digitalización y la permanencia del trabajo remoto.

Juan Carlos refirió que a pesar de ese panorama aún hay áreas de oportunidad que deben atenderse, como la necesidad de contar con una estrategia de ciberseguridad enfocada en la disminución de riesgos.

# VULNERABILIDADES RELEVANTES

# TABLA DE VULNERABILIDADES RELEVANTES: ABRIL 2023

| Identificador | Fecha de publicación | Título | CVSS v3.x | Referencias |
|---|---|---|---|---|
| CVE-2023-28697 | 04/26/2023 | Missing Authentication for Critical Function | CVSS v3.1:9.8 [critical] | https://nvd.nist.gov/vuln/detail/CVE-2023-25909 |

**Descripción:** Moxa MiiNePort E1 has a vulnerability of insufficient access control. An unauthenticated remote user can exploit this vulnerability to perform arbitrary system operation or disrupt service.

| Identificador | Fecha de publicación | Título | CVSS v3.x | Referencias |
|---|---|---|---|---|
| CVE-2023-20853 | 04/26/2023 | Deserialization of Untrusted Data | CVSS v3.1:9.8 [critical] | https://nvd.nist.gov/vuln/detail/CVE-2023-21058 |

**Descripción:** aEnrich Technology a+HRD has a vulnerability of Deserialization of Untrusted Data within its MSMQ asynchronized message process. An unauthenticated remote attacker can exploit this vulnerability to execute arbitrary system commands to perform arbitrary system operation or disrupt service.

| Identificador | Fecha de publicación | Título | CVSS v3.x | Referencias |
|---|---|---|---|---|
| CVE-2023-20852 | 04/24/2023 | Deserialization of Untrusted Data | CVSS v3.1:9.8 [critical] | https://nvd.nist.gov/vuln/detail/CVE-2022-42498 |

**Descripción:** aEnrich Technology a+HRD has a vulnerability of Deserialization of Untrusted Data within its MSMQ interpreter. An unauthenticated remote attacker can exploit this vulnerability to execute arbitrary system commands to perform arbitrary system operation or disrupt service.

| Identificador | Fecha de publicación | Título | CVSS v3.x | Referencias |
|---|---|---|---|---|
| CVE-2023-1020 | 04/24/2023 | Improper Neutralization of Special Elements | CVSS v3.1:9.8 [critical] | https://nvd.nist.gov/vuln/detail/CVE-2022-20532 |

**Descripción:** The Steveas WP Live Chat Shoutbox WordPress plugin through 1.4.2 does not sanitise and escape a parameter before using it in a SQL statement via an AJAX action available to unauthenticated users, leading to a SQL injection.

| Identificador | Fecha de publicación | Título | CVSS v3.x | Referencias |
|---|---|---|---|---|
| CVE-2023-30378 | 04/24/2023 | Out-of-bounds Write | CVSS v3.1:9.8 [critical] | https://nvd.nist.gov/vuln/detail/CVE-2023-28152 |

# TABLA DE VULNERABILIDADES RELEVANTES: ABRIL 2023

**Descripción:** In Tenda AC15 V15.03.05.19, the function "sub_8EE8" contains a stack-based buffer overflow vulnerability.

| Identificador | Fecha de publicación | Título | CVSS v3.x | Referencias |
|---|---|---|---|---|
| CVE-2023-20853 | 04/24/2023 | Deserialization of Untrusted Data | CVSS v3.1:9.8 [critical] | https://nvd.nist.gov/vuln/detail/CVE-2022-20532 |

**Descripción:** aEnrich Technology a+HRD has a vulnerability of Deserialization of Untrusted Data within its MSMQ asynchronized message process. An unauthenticated remote attacker can exploit this vulnerability to execute arbitrary system commands to perform arbitrary system operation or disrupt service.

| Identificador | Fecha de publicación | Título | CVSS v3.x | Referencias |
|---|---|---|---|---|
| CVE-2022-48477 | 04/24/2023 | Server-Side Request Forgery (SSRF) | CVSS v3.1:9.8 [critical] | https://nvd.nist.gov/vuln/detail/CVE-2023-28152 |

**Descripción:** In JetBrains Hub before 2023.1.15725 SSRF protection in Auth Module integration was missing.

| Identificador | Fecha de publicación | Título | CVSS v3.x | Referencias |
|---|---|---|---|---|
| CVE-2023-2245 | 04/22/2023 | Unrestricted Upload of File with Dangerous Type | CVSS v3.1:9.8 [critical] | https://nvd.nist.gov/vuln/detail/CVE-2023-2245 |

**Descripción:** Unrestricted Upload of File with Dangerous Type

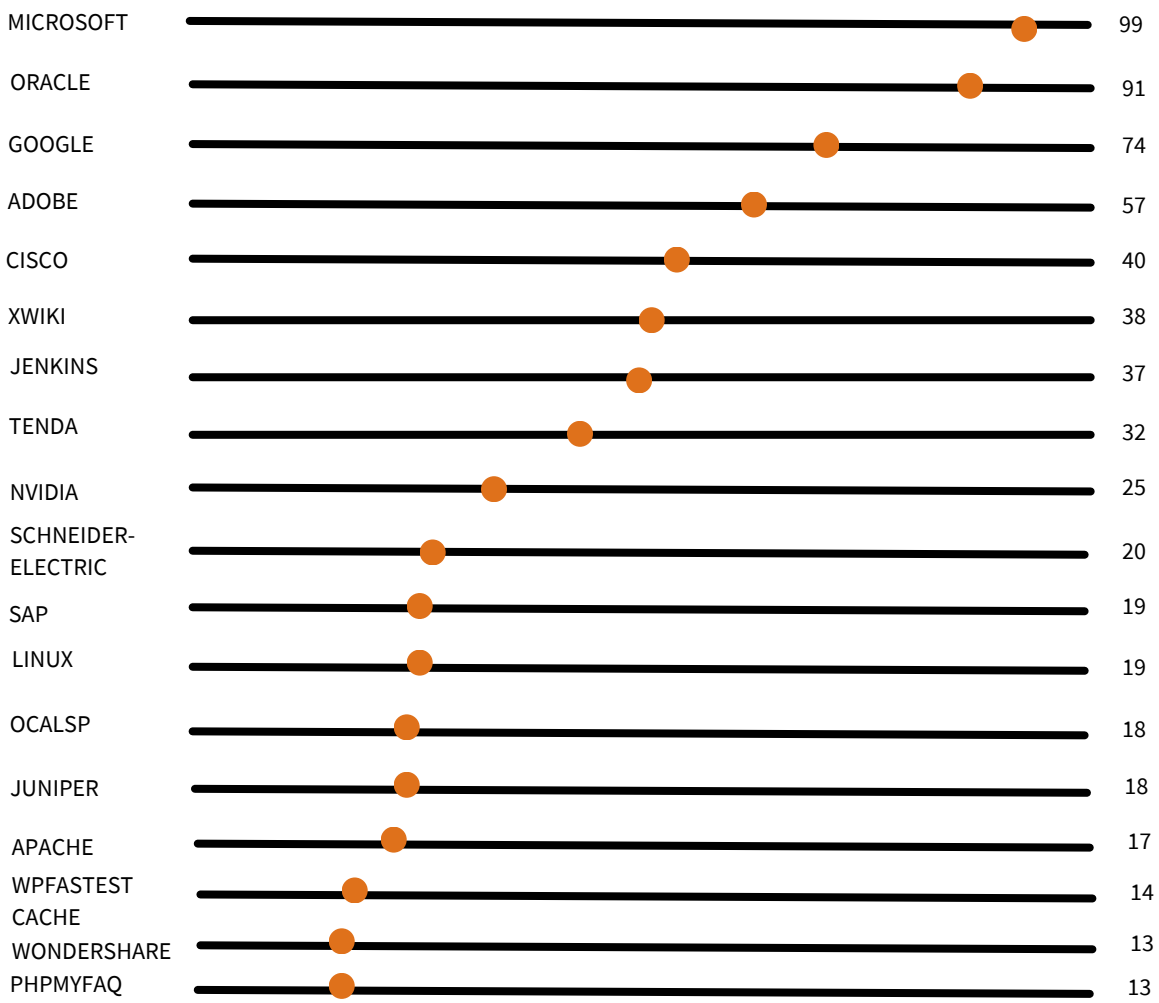
| Identificador | Fecha de publicación | Título | CVSS v3.x | Referencias |
|---|---|---|---|---|
| CVE-2023-23753 | 04/22/2023 | Improper Neutralization of Special Elements | CVSS v3.1:9.8 [critical] | https://nvd.nist.gov/vuln/detail/CVE-2022-28495 |

**Descripción:** The 'Visforms Base Package for Joomla 3' extension is vulnerable to SQL Injection as concatenation is used to construct an SQL Query. An attacker can interact with the database and could be able to read, modify and delete data on it.

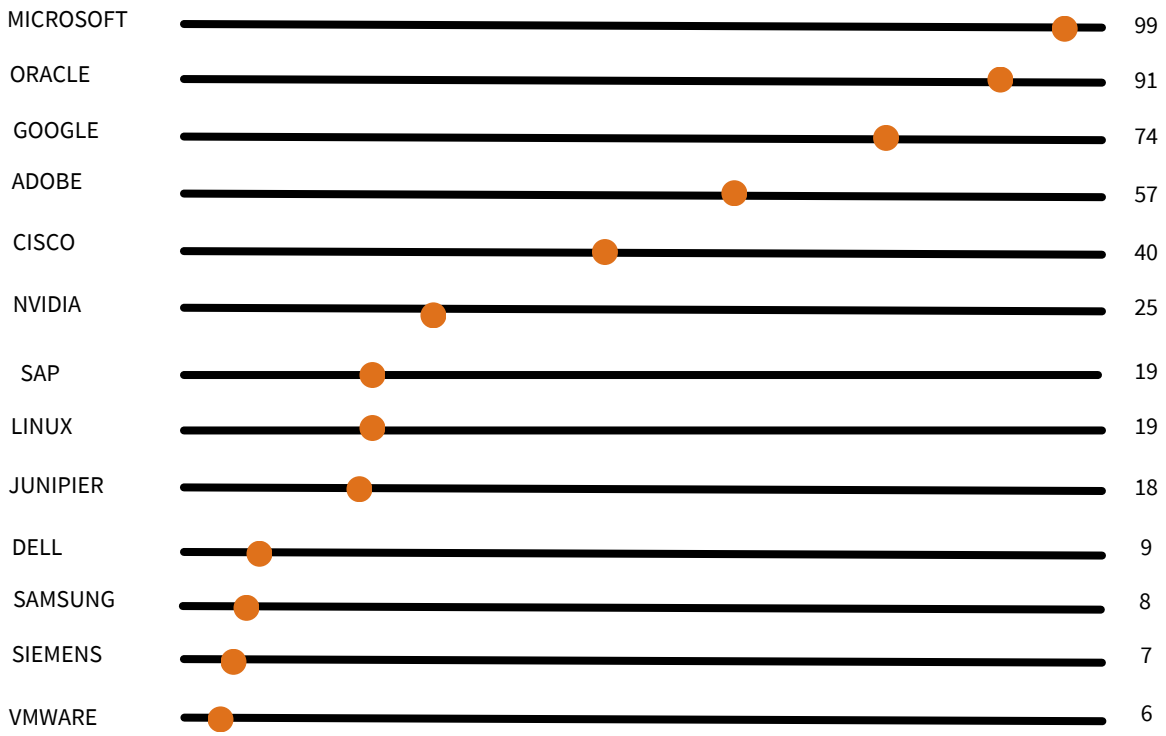
| Identificador | Fecha de publicación | Título | CVSS v3.x | Referencias |
|---|---|---|---|---|
| CVE-2023-2218 | 04/21/2023 | Improper Neutralization of Special Elements | CVSS v3.1:9.8 [critical] | https://nvd.nist.gov/vuln/detail/CVE-2023-2218 |

**Descripción:** A vulnerability has been found in SourceCodester Task Reminder System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/user/manage_user.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-226984.

# FABRICANTES Y SUS VULNERABILIDADES RELEVANTES: ABRIL DE 2023



# EMPRESAS MULTINACIONALES Y SUS VULNERABILIDADES: ABRIL DE 2023



# CULTURA DE CIBERSEGURIDAD

# TROYANO

Un virus troyano es un tipo de malware que se descarga en una computadora disfrazado de programa legítimo. El método de entrega suele hacer que un atacante utilice la ingeniería social generalmente vía correo electrónico para ocultar código malicioso dentro del software legítimo para intentar obtener acceso al sistema de los usuarios con su software, realizar diversas tareas, en la mayoría de los casos crean una puerta trasera (backdoor) que le permite la administración remota a un usuario no autorizado.

Las acciones que el atacante puede realizar en el equipo remoto dependen de los privilegios que tenga el usuario atacado en ese equipo y de las características del troyano. Para que un malware sea un troyano solo tiene que acceder y controlar la máquina anfitriona sin ser advertido, bajo una apariencia inocua.

Algunas de las operaciones más comunes que realiza son:

- Utilización la máquina como parte de una botnet (por ejemplo, para realizar ataques de denegación de servicio o envío de spam).
- Instalación de otros programas (incluyendo aplicaciones maliciosas).
- Robo de información personal: información bancaria, contraseñas, códigos de seguridad, robo de archivos varios, etcétera.
- Borrado, modificación o transferencia de archivos (descarga o subida).
- Borrado completo del disco.
- Ejecución o finalización de procesos.
- Apagado o reiniciado del equipo.
- Captura de las pulsaciones del teclado.
- Capturas de pantalla.
- Llenado del disco duro con archivos inútiles.
- Monitorización del sistema y seguimiento de las acciones del usuario.
- Captura de imágenes o videos a través de la webcam, si tiene.
- Acciones inocuas desde el punto de vista de la seguridad, destinadas a sorprender al usuario, tales como expulsar la unidad de CD, cambiar la apariencia del sistema, etc.

Actualmente, y dada la popularidad de los dispositivos móviles y tabletas, son estas plataformas (especialmente aquellas con menor control en su mercado de aplicaciones) las que suscitan un creciente interés entre los desarrolladores de este tipo de malware. Dado el uso personal de estos dispositivos, las acciones que un atacante puede realizar en estos dispositivos comprende las ya descritas, más otras específicas derivadas de la naturaleza privada de la información que se almacena en estas plataformas. Algunos ejemplos son:

- Captura de los mensajes entrantes y salientes de aplicaciones de mensajería.
- Captura del registro de llamadas.
- Acceso y modificación de contactos en la agenda.
- Habilidad para efectuar llamadas y enviar mensajes de texto.
- Conocimiento de la posición geográfica del dispositivo mediante GPS.

# TROYANOS

## FORMAS DE INFECTARSE CON TROYANOS

La mayoría de las infecciones con troyanos ocurren cuando se ejecuta un programa infectado con un troyano. Estos programas pueden ser de cualquier tipo, desde instaladores hasta presentaciones de fotos. Al ejecutar el programa, este se muestra y realiza las tareas de forma normal, pero en un segundo plano y al mismo tiempo se instala el troyano. El proceso de infección no es visible para el usuario ya que no se muestran ventanas ni alertas de ningún tipo, por lo que evitar la infección de un troyano es difícil. Algunas de las formas más comunes de infección son:.

- Descarga de programas de redes P2P.
- Páginas web que contienen contenido ejecutable (por ejemplo controles ActiveX o aplicaciones Java).
- Exploits para aplicaciones no actualizadas (navegadores, reproductores multimedia, clientes de mensajería instantánea).
- Ingeniería social (por ejemplo un cracker manda directamente el troyano a la víctima a través de la mensajería instantánea).
- Archivos adjuntos en correos electrónicos y archivos enviados por mensajería instantánea.
- Conectar a su equipo un dispositivo externo infectado.

## CÓMO EVITARLO

Debido a que cualquier programa puede realizar acciones maliciosas en un ordenador, hay que ser cuidadoso a la hora de ejecutarlos. Estos pueden ser algunos buenos consejos para evitar infecciones:

- Disponer de un programa antivirus actualizado regularmente para estar protegido contra las últimas amenazas.
- Disponer de un firewall correctamente configurado. Algunos antivirus lo traen integrado.
- Tener instalados los últimos parches y actualizaciones de seguridad del sistema operativo.
- Descargar los programas siempre de las páginas web oficiales o de páginas web de confianza.
- No abrir los datos adjuntos de un correo electrónico si no conoces al remitente.
- Evitar la descarga de software de redes p2p.
- Actualizar el software del equipo.

## CÓMO DETECTARLO

Debido a que cualquier programa puede realizar acciones maliciosas en un ordenador, hay que ser cuidadoso a la hora de ejecutarlos. Estos pueden ser algunos buenos consejos para evitar infecciones:

- Disponer de un programa antivirus actualizado regularmente para estar protegido contra las últimas amenazas.
- Disponer de un firewall correctamente configurado. Algunos antivirus lo traen integrado.
- Tener instalados los últimos parches y actualizaciones de seguridad del sistema operativo.
- Descargar los programas siempre de las páginas web oficiales o de páginas web de confianza. No abrir los datos adjuntos de un correo electrónico si no conoces al remitente.
- Evitar la descarga de software de redes p2p. Actualizar el software del equipo.

# TROYANOS

## COMO ELIMINARLOS

Una de las principales características de los troyanos es que no son visibles para el usuario. Un troyano puede estar ejecutándose en un ordenador durante meses sin que el usuario lo perciba. Esto hace muy difícil su detección y eliminación de forma manual. Algunos patrones para identificarlos son: un programa desconocido se ejecuta al iniciar el ordenador, se crean o borran archivos de forma automática, el ordenador funciona más lento de lo normal, errores en el sistema operativo.


Por otro lado, los programas antivirus están diseñados para eliminar todo tipo de software malicioso, además de eliminarlos también previenen de nuevas infecciones actuando antes de que el sistema resulte infectado. Es muy recomendable tener siempre un antivirus instalado en el equipo y a ser posible también un firewall.

# REFERENCIAS

# REFERENCIAS


- https://patchstack.com/articles/psa-houzez-theme-unauthenticated-privileRoyal+Ransomwarege-escalation-vulnerability-exploited-in-the-wild/
- https://blog.lumen.com/new-hiatusrat-router-malware-covertly-spies-on-victims/
- https://www.hyas.com/blog/blackmamba-using-ai-to-generate-polymorphic-malware
- https://www.threatfabric.com/blogs/xenomorph-v3-new-variant-with-ats.html
- https://blog.talosintelligence.com/yorotrooper-espionage-campaign-cis-turkey-europe/
- https://www.akamai.com/blog/security-research/hinatabot-uncovering-new-golang-ddos-botnet
- https://www.kaspersky.com/blog/chatgpt-stealer-win-client/47274/
- https://heraldodemexico.com.mx/nacional/2023/2/2/hackean-al-buro-de-credito-descubren-venta-de-la-informacion-de-los-clientes-en-redes-sociales-478457.html

# ZERU

Cybersecurity Services

Security Operation Center - SOC by

ADV


+52 55 6178 9397

contacto@adv-ic.com

Av. Melchor Ocampo 193, Torre Privanza, Piso 11 Oficina 11D
Colonia Veronica Anzures. Delegación Miguel Hidalgo CP 11300