# BOLETÍN INFORMATIVO

003–2022

# CONCIBER

Comité Nacional de Seguridad Cibernética

## Limitación de Responsabilidad

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Comité Nacional de Seguridad Cibernética - CONCIBER puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

## Aviso Legal

## Contenido

## Comité Nacional de Seguridad Cibernética – CONCIBER:

Por medio de este boletín informativo destacamos las noticias más relevantes en el ámbito de la ciberseguridad, en cuanto a las vulnerabilidades Altas y Críticas, que impactan especialmente en las tecnologías empleadas en el sector público y privado.

El Centro Estratégico de Monitoreo - CEM trabaja constantemente en la recopilación y clasificación de las nuevas vulnerabilidades, realizando un análisis teórico y técnico cuando sea posible, de aquellas que por su nivel de criticidad lo requieran.

La publicación de dichas noticias dependerá de la importancia y calidad informativa de las mismas. A su vez se incluyen referencias técnicas y de gestión a los efectos de reducir los riesgos con anticipación y adecuada planificación.

# Vulnerabilidades Tecnológicas

## Vulnerabilidad Zero-day en Microsoft Exchange

**Ponderación CVSSv3:**

Crítica

**Descripción:**

Microsoft alerta de la detección de dos vulnerabilidades zero-day, catalogadas como CVE-2022-41040 y CVE-2022-41082, que afectan a Microsoft Exchange Server 2013, 2016 y 2019. Dichas vulnerabilidades estarían siendo utilizadas por actores de amenazas para comprometer servidores vulnerables.

Los expertos revelaron que las solicitudes utilizadas en esta cadena de explotación son similares a las utilizadas en los ataques dirigidos a las vulnerabilidades de ProxyShell, por lo que se les conoce como ProxyNotShell.

La vulnerabilidad CVE-2022-41040 es de tipo Server Side Request Forgery (SSRF), mientras que la segunda, identificada como CVE-2022-41082 permite la ejecución remota de código (RCE). Para que la explotación sea exitosa es necesario disponer de credenciales válidas para el acceso al servidor Exchange vulnerable.

La base de datos del NIST aún ha registrado las vulnerabilidades descritas anteriormente, por lo que todavía no cuentan con una valoración según asignando la escala CVSSv3. Sin embargo, el fabricante ha identificado las vulnerabilidades con los CVE-2022-41040 y CVE-2022-41082, y les ha otorgado una severidad crítica.

**Recursos afectados**

Microsoft Exchange Server versiones: 2013, 2016 y 2019.

**Recomendaciones:**

Microsoft ha publicado un aviso donde indica que bloquear los puertos remotos de PowerShell (HTTP: 5985 y HTTPS: 5986) puede limitar la explotación de la vulnerabilidad. También indica una posible mitigación, consistente en agregar una regla de bloqueo para bloquear los patrones de ataque conocidos.

Se recomienda encarecidamente a los usuarios y administradores de sistemas que apliquen las medidas alternativas expuestas por Microsoft, con el fin de evitar la exposición a ataques externos y la toma de control de los sistemas informáticos.

**Fuentes de referencia:**

https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/
https://www.microsoft.com/security/blog/2022/09/30/analyzing-attacks-using-the-exchange-vulnerabilities-cve-2022-41040-and-cve-2022-41082/
https://www.cronup.com/alerta-de-seguridad-nueva-vulnerabilidad-critica-para-microsoft-exchange-en-explotacion-activa-0-day-rce/

**Vulnerabilidad crítica en el administrador de contenidos Drupal Core**

**Ponderación CVSSv3:**

Crítica

**Descripción:**

Drupal utiliza la biblioteca de terceros Twig para la limpieza y la creación de plantillas de contenido. Twig ha lanzado una actualización de seguridad que afecta a Drupal,la vulnerabilidad ha sido calificada como crítica.

El código del núcleo de Drupal que extiende Twig también se ha actualizado para mitigar una vulnerabilidad relacionada.

Son posibles múltiples vulnerabilidades si un usuario que no es de confianza tiene acceso para escribir código Twig, incluido el posible acceso de lectura no autorizado a archivos privados, el contenido de otros archivos en el servidor o las credenciales de la base de datos.

La vulnerabilidad se ve mitigada por el hecho de que un exploit solo es posible en el núcleo de Drupal con un permiso administrativo de acceso restringido. Pueden existir rutas de explotación adicionales para la misma vulnerabilidad con código contribuido o personalizado que permite a los usuarios escribir plantillas Twig.

**Recursos Afectados**

Drupal core: >= 8.0.0 = 9.4.0

Todas las versiones de Drupal 9 anteriores a 9.3.x están al final de su ciclo de vida y no reciben cobertura de seguridad. Tenga en cuenta que Drupal 8 ha llegado al final de su vida útil .

El núcleo de Drupal 7 no incluye Twig y, por lo tanto, no se ve afectado

**Recomendaciones:**

Instale la última versión para los producos:

Si está utilizando Drupal 9.4, actualice a Drupal 9.4.7 .
Si está utilizando Drupal 9.3, actualice a Drupal 9.3.22 .

.

**Fuentes de referencia:**

https://www.drupal.org/sa-core-2022-016
https://www.ccn-cert.cni.es/seguridad-al-dia/vulnerabilidades/view/33735.html

**Vulnerabilidad en la herramienta OpenSSH**

**Ponderación CVSSv3:**

Crítica

**Descripción:**

La herramienta de conectividad para el inicio de sesión remoto que usa el protocolo SSH es propensa a una vulnerabilidad de enumeración de usuarios debido a que no retrasa el rescate de un usuario autenticado no válido hasta después de que el paquete que contiene la solicitud se haya analizado por completo, relacionado con auth2-gss.c, auth2-hostbased.c y auth2-pubkey .C. ( CVE-2018-15473 )

Un atacante puede explotar esta vulnerabilidad para obtener acceso al sistema afectado.

**Recursos afectados**

OpenSSH hasta la versión 7.7

**Recomendaciones:**

Para determinar si su producto y versión han sido evaluados para esta vulnerabilidad, consulte el cuadro para determinar si se sabe que su versión es vulnerable, los componentes o características que se ven afectados por la vulnerabilidad y para obtener información sobre las versiones o las revisiones que abordan la vulnerabilidad, consulte la siguiente tabla https://support.f5.com/csp/article/K51812227

Si está ejecutando una versión que figura en la columna Versiones conocidas como vulnerables, puede eliminar esta vulnerabilidad actualizando a una versión que figura en la columna Correcciones introducidas en . Si la tabla enumera solo una versión anterior a la que está ejecutando actualmente, o no enumera una versión no vulnerable, entonces no existe ningún candidato de actualización actualmente

**Fuentes de referencia:**

https://support.f5.com/csp/article/K51812227
https://www.ccn-cert.cni.es/seguridad-al-dia/vulnerabilidades/view/33732.html

## Vulnerabilidad en los productos Oracle Java SE y Oracle GraalVM Enterprise Edition de Oracle Java SE

**Ponderación CVSSv3:**

Alta

**Descripción:**

Esta vulnerabilidad es fácilmente explotable permite que un atacante no autenticado con acceso a la red a través de múltiples protocolos comprometa Oracle Java SE, Oracle GraalVM Enterprise Edition. Los ataques exitosos de esta vulnerabilidad pueden resultar en actualizaciones no autorizadas, inserción o eliminación del acceso a algunos de los datos accesibles de Oracle Java SE, Oracle GraalVM Enterprise Edition.

Esta vulnerabilidad se aplica a las implementaciones de Java, generalmente en clientes que ejecutan aplicaciones Java Web Start en espacio aislado o subprogramas Java en espacio aislado, que cargan y ejecutan código que no es de confianza (por ejemplo, código que proviene de Internet) y confíe en la zona de pruebas de Java para su seguridad. Esta vulnerabilidad también se puede explotar mediante el uso de API en el Componente especificado, por ejemplo, a través de un servicio web que proporciona datos a las API.

**Recursos afectados**

Las versiones compatibles que se ven afectadas son Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 y 21.3.0.

**Recomendaciones:**

El fabricante recomiendo encarecidamente a todos los usuarios de OpenJDK actualizar los productos a la última versión disponible para mitigar el incidente.

**Fuentes de referencia:**

https://nvd.nist.gov/vuln/detail/CVE-2022-21291
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21291
https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/2DIN3L6L3SVZK75CKW2GPSU4HIGZR7XG/
https://security.gentoo.org/glsa/202209-05
https://security.netapp.com/advisory/ntap-20220121-0007/
https://www.debian.org/security/2022/dsa-5057
https://www.debian.org/security/2022/dsa-5058
https://www.oracle.com/security-alerts/cpujan2022.html

## Múltiples vulnerabilidades de MySQL (CVE-2020-26237, CVE-2021-22119, CVE-2022-1292, CVE-2022-21455, CVE-2022-21509)

**Ponderación CVSSv3:**

Alto

**Descripción:**

CVE-2020-26237
Highlight.js es un resaltador de sintaxis escrito en JavaScript, actualmente es vulnerable a la contaminación de prototipos. Se puede crear un bloque de código HTML malicioso que provocará la contaminación del prototipo del objeto base durante el resaltado. Si permite que los usuarios inserten bloques de código HTML personalizados en su página/aplicación mediante el análisis de bloques de código Markdown (o similar) y no filtra los nombres de idioma que el usuario puede proporcionar, es posible que sea vulnerable. La contaminación debería ser solo datos inofensivos, pero esto puede causar problemas para las aplicaciones que no esperan que existan estas propiedades y puede provocar un comportamiento extraño o bloqueos de la aplicación, es decir, un vector potencial de DOS.

CVE-2021-22119
La vulnerabilidad existente en el producto Spring Security es susceptibles a una denegación de servicio (DoS) ataque a través del inicio de la Solicitud de Autorización en una aplicación OAuth 2.0 Client Web y WebFlux. Un usuario o atacante malintencionado puede enviar múltiples solicitudes iniciando la Solicitud de autorización para la concesión del código de autorización, lo que tiene el potencial de agotar los recursos del sistema utilizando una sola sesión o varias sesiones.

CVE-2022-1292
Vulnerabilidad en el script c_rehash, no desinfecta correctamente los metacaracteres del shell para evitar la inyección de comandos. Este script es distribuido por algunos sistemas operativos de manera que se ejecuta automáticamente. En dichos sistemas operativos, un atacante podría ejecutar comandos arbitrarios con los privilegios del script. El uso del script c_rehash se considera obsoleto.

CVE-2022-21455
Vulnerabilidad en el producto MySQL Server de Oracle MySQL (componente: Server: PAM Auth Plugin). La vulnerabilidad fácilmente explotable permite que un atacante con privilegios altos con acceso a la red a través de múltiples protocolos comprometa el servidor MySQL. Los ataques exitosos de esta vulnerabilidad pueden resultar en la creación, eliminación o modificación del acceso no autorizado a datos críticos o a todos los datos accesibles del servidor MySQL.

CVE-2022-21509
La vulnerabilidad en el producto MySQL Server de Oracle MySQL (componente: Server: Optimizer)fácilmente explotable permite que un atacante con privilegios altos con acceso a la red a través de múltiples protocolos comprometa el servidor MySQL. Los ataques exitosos de esta vulnerabilidad pueden dar lugar a la capacidad no autorizada de provocar un bloqueo o un bloqueo repetible (DOS completo) del servidor MySQL, así como la actualización, inserción o eliminación no autorizadas del acceso a algunos de los datos accesibles del servidor MySQL.

**Recursos afectados**

- Highlight.js anteriores a la 9.18.2 y la 10.1.2
- Spring Security 5.5.x anteriores a 5.5.1, 5.4.x anteriores a 5.4.7, 5.3.x anteriores a 5.3.10 y 5.2.x anteriores a 5.2.11
- y debe reemplazarse por la herramienta de línea de comandos de rehash de OpenSSL. Corregido en OpenSSL 3.0.3 (Afectado 3.0.0,3.0.1,3.0.2). Corregido en OpenSSL 1.1.1o (Afectado 1.1.1-1.1.1n). Corregido en OpenSSL 1.0.2ze (Afectado 1.0.2-1.0.2zd).
- Las versiones compatibles en MySQL Server de Oracle MySQL (componente: Server: PAM Auth Plugin) que se ven afectadas son la 8.0.28 y anteriores.
- Las versiones compatibles que se ven afectadas son la 8.0.29 y anteriores del producto MySQL Server de Oracle MySQL (componente: Server: Optimizer).

**Recomendaciones:**

- El fabricante recomienda encarecidamente que se actualicen todos los productos que se mencionan en este apartado a una versión más reciente.
- En el caso del script c_rehash debe reemplazarse por la herramienta de línea de comandos de rehash de OpenSSL (CVE-2021-22119).

**Fuentes de referencia:**

https://nvd.nist.gov/vuln/detail/CVE-2020-26237
https://support.f5.com/csp/article/K62444703

## Vulnerabilidad en Procesadores Intel® Xeon®

**Ponderación CVSSv3:**

Alto

**Descripción:**

Una posible vulnerabilidad de seguridad en el firmware del BIOS para algunos procesadores Intel® puede permitir la escalada de privilegios.La escritura fuera de los límites en el firmware del BIOS para algunos procesadores Intel(R) puede permitir que un usuario autenticado habilite potencialmente la escalada de privilegios a través del acceso local.

**Recursos afectados**

Familia de procesadores escalables Intel® Xeon® de tercera generación (CPU 5065B, 606A0, 606A4, 606A6)

**Recomendaciones:**

Intel recomienda que los usuarios de procesadores Intel® actualicen a la última versión proporcionada por el fabricante del sistema que soluciona estos problemas.

**Fuentes de referencia:**
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00686.html

**Múltiples vulnerabilidades del kernel de Linux (CVE-2019-6454, CVE-2020-12888, CVE-2020-36385)**

**Ponderación CVSSv3:**

Alto

**Descripción:**

CVE-2019-6454 Se descubrió que systemd asigna un búfer lo suficientemente grande como para almacenar el campo de ruta de un mensaje dbus sin realizar suficientes comprobaciones. Un atacante local puede desencadenar esta falla al enviar un mensaje dbus a systemd con una ruta grande que hace que systemd se bloquee o posiblemente eleve sus privilegios.

CVE-2020-12888 Este vulnerabilidad afecta a las versiones del paquete del kernel que se envían con Red Hat Enterprise Linux.

CVE-2020-36385 Las versiones del Kernel de Linux anteriores a la 5.10 son susceptibles a una vulnerabilidad que, cuando se aprovecha con éxito, podría dar lugar a la divulgación de información confidencial, la adición o modificación de datos o la denegación de servicio (DoS).

**Recursos afectados**

- CVE-2019-6454 – versiones de Red Hat Virtualization Hypervisor and Management Appliance (Linux versiones 7 y 8)
- CVE-2020-12888 – Versiones de Red Hat Enterprise (versiones de linux 5, 6, 7, 8)
- CVE-2020-36385 - Versiones del Kernel de Linux anteriores a la 5.10

**Recomendaciones:**

- Para corregir las vulnerabilidades del CVE-2019-6454, CVE-2020-12888, CVE-2020-36385 deben aplicarse de inmediato los parches publicados por el fabricante.

**Fuentes de referencia:**

https://access.redhat.com/security/cve/cve-2019-6454
https://access.redhat.com/security/cve/cve-2020-12888
https://www.rapid7.com/db/vulnerabilities/centos_linux-cve-2020-36385/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-36385

**Vulnerabilidad NGINX ModSecurity WAF (CVE-2021-42717)**

**Ponderación CVSSv3:**

Alto

**Descripción:**

Se encontró una falla en glibc. Un desbordamiento y subdesbordamiento del búfer de uno en uno en getcwd() puede provocar daños en la memoria cuando el tamaño del búfer es exactamente 1. Un atacante local que pueda controlar el búfer de entrada y el tamaño pasado a getcwd() en un programa setuid podría use esta falla para ejecutar potencialmente código arbitrario y escalar sus privilegios en el sistema.

**Recursos afectados**

- Red Hat Enterprise Linux para x86_64 8 x86_64
- Red Hat Enterprise Linux para x86_64 - Soporte de actualización extendido 8.6 x86_64
- Servidor Red Hat Enterprise Linux - AUS 8.6 x86_64
- Red Hat Enterprise Linux para IBM z Systems 8 s390x
- Red Hat Enterprise Linux para IBM z Systems - Soporte de actualización extendido 8.6 s390x
- Red Hat Enterprise Linux para Power, little endian 8 ppc64le
- Red Hat Enterprise Linux para Power, little endian - Soporte de actualización extendido 8.6 ppc64le
- Red Hat Virtualization Host 4 para RHEL 8 x86_64
- Servidor Red Hat Enterprise Linux - TUS 8.6 x86_64
- Red Hat Enterprise Linux para ARM 64 8 aarch64
- Red Hat Enterprise Linux para ARM 64 - Soporte de actualización extendido 8.6 aarch64
- Red Hat CodeReady Linux Builder para x86_64 8 x86_64
- Red Hat CodeReady Linux Builder para Power, little endian 8 ppc64le
- Red Hat CodeReady Linux Builder para ARM 64 8 aarch64
- Red Hat CodeReady Linux Builder para IBM z Systems 8 s390x
- Red Hat CodeReady Linux Builder para x86_64 - Soporte de actualización extendido 8.6 x86_64
- Red Hat CodeReady Linux Builder for Power, little endian - Soporte de actualización extendido 8.6 ppc64le
- Red Hat CodeReady Linux Builder para IBM z Systems - Soporte de actualización extendida 8.6 s390x
- Red Hat CodeReady Linux Builder para ARM 64 - Soporte de actualización extendido 8.6 aarch64

**Recomendaciones:**

Deben aplicarse los parches de actualización publicados por el fabricante y para que los mismos surtan efectos, se deben reiniciar todos los servicios vinculados a la biblioteca glibc o reiniciar el sistema.

**Fuentes de referencia:**

https://access.redhat.com/errata/RHSA-2022:0896