Hasta el 8 de febrero

# AVISOS TÉCNICOS

EUSKO JAURLARITZA
GOBIERNO VASCO

cyber zaintza

# Inyección SQL en Ivanti Endpoint Manager

Ivanti ha descubierto una vulnerabilidad crítica en su producto EPM (Endpoint Manager), de tipo inyección SQL, cuya explotación podría permitir a un atacante remoto ejecutar código.

Avisos técnicos - Hasta el 8 de febrero

# Vulnerabilidad de ruta trasversal en OpManager de ManageEngine

Marcin 'Icewall' Noga de Cisco Talos, ha descubierto una vulnerabilidad de severidad crítica que podría provocar un cruce de directorio en la funcionalidad uploadMib.

Avisos técnicos - Hasta el 8 de febrero

# Vulnerabilidad de desbordamiento de búfer en XAMPP

INCIBE ha coordinado la publicación de una vulnerabilidad que afecta a XAMPP de Apachefriends en sus versiones 8.2.4 y anteriores, la cual ha sido descubierta por Rafael Pedrero.

A esta vulnerabilidad se le ha asignado la siguiente puntuación base CVSS v3.1, vector del CVSS y tipo de vulnerabilidad CWE:

CVE-2024-0338: CVSS v3.1: 7.3 | CVSS: AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H | CWE-119.

Avisos técnicos - Hasta el 8 de febrero

# Actualización de seguridad de SAP-Enero 2024

SAP ha publicado las actualizaciones de seguridad correspondientes al mes de enero para una amplia gama de sus productos. En total, se han notificado 10 nuevas notas de seguridad, a las que se añaden 2 actualizaciones de notas publicadas con anterioridad

Avisos técnicos - Hasta el 8 de febrero

# Actualización de seguridad de Android-Enero 2024

Google ha publicado las actualizaciones de seguridad de Android y dispositivos Píxel del mes de enero de 2024, en donde se corrigen 61 vulnerabilidades, abarcando soluciones para fallos de elevación de privilegios, divulgación de información y ejecución remota de código.

Avisos técnicos - Hasta el 8 de febrero

# Actualización de seguridad de Microsoft-Enero 2024

Microsoft ha publicado las actualizaciones de seguridad del mes de enero de 2024 en las que se corrigen 54 vulnerabilidades, siendo 2 de ellas calificadas como críticas, 47 como importantes y 5 sin un valor asignado que afectan al navegador Edge basado en Chromium.

Estas vulnerabilidades afectan a productos como Visual Studio, Windows Group Policy, Microsoft Virtual Hard Drive, Windows Message Queuing, .NET Core & Visual Studio, Windows Authentication Methods, Azure Storage Mover, Microsoft Office, Windows Subsystem for Linux, Windows Cryptographic Services, entre otros.

## Avisos técnicos - Hasta el 8 de febrero

# Vulnerabilidad de denegación de servicio en Squid

Auscert ha publicado una vulnerabilidad de severidad crítica que podría provocar una denegación de servicio en la herramienta afectada.

Avisos técnicos - Hasta el 8 de febrero

# Vulnerabilidad de alto impacto en FortiOS y FortiProxy

Fortinet ha publicado un aviso de seguridad para tratar 1 vulnerabilidad de severidad alta, con el identificador CVE-2023-44250, que afecta a los productos FortiOS y FortiProxy. Esta vulnerabilidad supone una amenaza de alta gravedad para la confidencialidad, interidad y disponibilidad de los sistemas que se puedan ver afectados.

Avisos técnicos - Hasta el 8 de febrero

# Actualización de seguridad de SAP de enero de 2024

SAP ha publicado varias actualizaciones de seguridad en diferentes productos en su comunicado mensual.

## Avisos técnicos - Hasta el 8 de febrero

# Actualizaciones de seguridad de Microsoft de enero de 2024

La publicación de actualizaciones de seguridad de Microsoft, correspondiente a la publicación de vulnerabilidades del 10 de enero, consta de 48 vulnerabilidades (con CVE asignado), calificadas 2 como críticas, 26 como importantes y como 20 medias.

Avisos técnicos - Hasta el 8 de febrero

# Múltiples vulnerabilidades en productos FireEye

INCIBE ha coordinado la publicación de 7 vulnerabilidades que afectan a múltiples productos de FireEye, las cuales han sido descubiertas por Albert Sánchez Miñano.

Avisos técnicos - Hasta el 8 de febrero

# Vulnerabilidad de desbordamiento de buffer en Hex Workshop

INCIBE ha coordinado la publicación de una vulnerabilidad de severidad alta que afecta a Hex Workshop versión 6.7 (6.8.0.5419 / Sep 1 2014), la cual ha sido descubierta por Rafael Pedrero.

A esta vulnerabilidad se le ha asignado el siguiente código, puntuación base CVSS v3.1, vector del CVSS y el tipo de vulnerabilidad CWE:

CVE-2022-0003: 7.3 | CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H | CWE-119.

Avisos técnicos - Hasta el 8 de febrero

# Vulnerabilidades de alto impacto en productos de Ivanti

Ivanti ha publicado un aviso de seguridad para tratar dos vulnerabilidades, CVE-2024-21887 de inyección de comando y severidad crítica y CVE-2023-46805 de omisión de autenticación y severidad alta. Estos errores afectan a los productos Ivanti Policy Secure Gateways e Ivanti Connect Secure, respectivamente. Los fallos podrían suponer una amenaza de gravedad crítica para varios productos de Ivanti con impacto en la confidencialidad de los sistemas que se vean afectados.

Avisos técnicos - Hasta el 8 de febrero

# Múltiples vulnerabilidades en productos Ivanti

Ivanti ha publicado dos vulnerabilidades, una de severidad crítica y otra de severidad alta, afectan potencialmente a cualquier empresa o usuario que esté utilizando los productos afectados, las cuales están siendo explotadas desde diciembre de 2023.

Avisos técnicos - Hasta el 8 de febrero

# Vulnerabilidad crítica en Cisco Unity Connection

ICisco ha publicado un aviso de seguridad para tratar una vulnerabilidad, de severidad critica, que afecta a la interfaz web de gestión de Cisco Unity Connection. El identificador de este error, que podría permitir a un atacante remoto no autenticado cargar archivos arbitrarios en un sistema afectado y ejecutar comandos en el sistema operativo subyacente, es el CVE-2024-20272.

Avisos técnicos - Hasta el 8 de febrero

# Vulnerabilidades en Google Chrome

Google ha publicado un aviso de seguridad actualizando el canal de asistencia a largo plazo para ChromeOS, donde se corrigen 5 vulnerabilidades de las cuales 2 son consideradas con una severidad alta, cuyos identificadores son CVE-2023-7024, ya tratada en un aviso anterior, y CVE-2023-5197. Las 3 restantes se consideran como de severidad media con los identificadores CVE-2023-5851, CVE-2023-5852, CVE-2023-5855.

Avisos técnicos - Hasta el 8 de febrero

# Múltiples vulnerabilidades en WIC1200 de Full Compass Systems

INCIBE ha coordinado la publicación de 3 vulnerabilidades de severidad alta que afectan a WIC1200 versión 1.1, un dispositivo hardware para administración de sitios web, las cuales han sido descubiertas por HADESS.

A estas vulnerabilidades se le han asignado los siguientes códigos, puntuación base CVSS v3.1, vector del CVSS y el tipo de vulnerabilidad CWE de cada vulnerabilidad:

| | | |
|---|---|---|
| CVE-2024-0554: | 5.5 | CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:L | CWE-79. |
| CVE-2024-0555: | 4.6 | CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:L | CWE-352. |
| CVE-2024-0556: | 7.1 | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N | CWE-261. |

## Avisos técnicos - Hasta el 8 de febrero

# Consumo de recursos en scdbg de Sandsprite

INCIBE ha coordinado la publicación de una vulnerabilidad de severidad alta que afecta a scdbg v1.0, una herramienta para analizar código shell, la cual ha sido descubierta por Rafael Pedrero.

A esta vulnerabilidad se le ha asignado el siguiente código, puntuación base CVSS v3.1, vector del CVSS y el tipo de vulnerabilidad CWE:

CVE-2024-0581: 7.5 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H | CWE-400.

Avisos técnicos - Hasta el 8 de febrero

# Omisión de autorización mediante clave controlada en Qsige

INCIBE ha coordinado la publicación de una vulnerabilidad de severidad media que afecta a QSige de IDSistemas, un sistema inteligente de gestión de esperas y colas, la cual ha sido descubierta por Oscar Atienza.

A esta vulnerabilidad se le ha asignado el siguiente código, puntuación base CVSS v3.1, vector del CVSS y el tipo de vulnerabilidad CWE:

CVE-2024-0580: 6.5 | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N | CWE-639.

Avisos técnicos - Hasta el 8 de febrero

# [Actualización 17/01/2024] Múltiples vulnerabilidades en productos de Atlassian

Atlasian ha publicado su boletín de seguridad con 28 vulnerabilidades de gravedad alta, de las cuales destacan dos (CVE-2023-22526 y CVE-2024-21672), que podrían permitir la ejecución remota de código en el centro de datos y el servidor de Confluence.

Avisos técnicos - Hasta el 8 de febrero

# Vulnerabilidad crítica VMware Aria Automation

VMware ha publicado un aviso de seguridad para tratar una vulnerabilidad, de severidad critica, que afecta a la herramienta VMware Aria Automation.

El identificador de este error, que podría permitir a un actor malicioso acceso no autorizado a organizaciones y flujos de trabajo remotos, es el CVE-2023-34063, que, de ser explotado supondría una amenaza de alta gravedad para la integridad y disponibilidad de los sistemas.

Avisos técnicos - Hasta el 8 de febrero

# Vulnerabilidades en NetScaler ADC y NetScaler Gateway

Citrix ha publicado un aviso de seguridad donde se abordan dos nuevas vulnerabilidades, de las cuales una se evalúa con una severidad alta cuyo identificador es CVE-2023-6549 y que conduce a una condición de denegación de servicios. Por otra parte, se reporta la vulnerabilidad con identificador CVE-2023-6548 y severidad media de ejecución remota de código.

Avisos técnicos - Hasta el 8 de febrero

# Múltiples vulnerabilidades en productos de Cires21

INCIBE ha coordinado la publicación de 2 vulnerabilidades de severidad crítica que afectan a Cires21 Live Encoder y Live Mosaic, versión 5.3, una solución para la grabación de parrillas completas de canales de televisión, las cuales han sido descubiertas por Konrad Kowal Karp.

Avisos técnicos - Hasta el 8 de febrero

# Fatal de control de acceso en VMware Aria Automation

Vmware ha publicado una vulnerabilidad de severidad crítica que podría provocar el acceso no autorizado a organizaciones y flujos de trabajo remotos.

Avisos técnicos - Hasta el 8 de febrero

# Vulnerabilidad de desbordamiento de búfer en Explorer++

INCIBE ha coordinado la publicación de una vulnerabilidad de severidad alta que afecta a Explorer++.exe, versión 1.3.5.531, un gestor de archivos ligero y rápido para Windows, la cual ha sido descubierta por Rafael Pedrero.

A esta vulnerabilidad se le ha asignado el siguiente código, puntuación base CVSS v3.1, vector del CVSS y el tipo de vulnerabilidad CWE:

| | | |
|---|---|---|
| CVE-2024-0645: | 7.3 | |
| CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H | | |
| CWE-119 | | |

Avisos técnicos - Hasta el 8 de febrero

# Vulnerabilidades de alto impacto en productos de Atlassian

Atlassian ha publicado su actualización de seguridad mensual donde se tratan múltiples vulnerabilidades de severidad alta que afectan a los productos Bitbucket Data Center, Bitbucket Server, Bamboo Data Center y Server, Jira Data Center y Server, Jira Service Management Data Center y Server, Crowd Data Center y Server, Confluence Data Center y Confluence Server.

Avisos técnicos - Hasta el 8 de febrero

# Vulnerabilidad en el Core de Drupal (módulo Comment)

Drupal ha lanzado una actualización de seguridad, para abordar la corrección de un fallo de severidad alta que afecta al core de Drupal, en el módulo Comment.

La explotación de esta vulnerabilidad conduce a condiciones de denegación de servicio sin tener impacto en la confidencialidad ni la integridad de los sistemas.

Avisos técnicos - Hasta el 8 de febrero

# Múltiples vulnerabilidades en cajeros Bitcoin ATM Douro de Lamassu

INCIBE ha coordinado la publicación de 3 vulnerabilidades de severidad media que afectan a los cajeros bitcoin ATM Douro del fabricante Lamassu en su versión 7.1, las cuales han sido descubiertas por Gabriel González.

Avisos técnicos - Hasta el 8 de febrero

# Cross-Frame Scripting (XFS) en Plone CMS

INCIBE ha coordinado la publicación de una vulnerabilidad de severidad media, que afecta a Plone CMS 6.0.5, un gestor de contenido, la cual ha sido descubierta por Miguel Segovia Gil.

A esta vulnerabilidad se le ha asignado el siguiente código, puntuación base CVSS v3.1, vector del CVSS y el tipo de vulnerabilidad CWE:

CVE-2024-0669:6.3 | AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L | CWE-1021.

Avisos técnicos - Hasta el 8 de febrero

# Vulnerabilidades de severidad alta en Google Chrome

Google ha emitido un aviso de seguridad actualizando el canal estable para la mayoría de dispositivos ChromeOS, donde se corrigen 5 vulnerabilidades de severidad alta con los identificadores CVE-2023-6706, CVE-2023-6703, CVE-2023-6508, CVE-2024-0519, CVE-2023-4969.

Avisos técnicos - Hasta el 8 de febrero

# Actualización de seguridad de Oracle-Enero 2024

Oracle ha publicado su boletín trimestral de actualizaciones de seguridad, que aborda 398 correcciones en una amplia variedad de productos. La mayoría de estos fallos permiten a un atacante remoto comprometer la integridad, confidencialidad y disponibilidad de los sistemas afectados, lo que podría dar lugar a la pérdida de datos y la interrupción de los servicios.

Avisos técnicos - Hasta el 8 de febrero

# Actualizaciones críticas en Oracle (enero 2024)

Oracle ha publicado una actualización crítica con parches para corregir vulnerabilidades, que afectan a múltiples productos.

## Avisos técnicos - Hasta el 8 de febrero

# Múltiples vulnerabilidades en Cups Easy

INCIBE ha coordinado la publicación de 42 vulnerabilidades de severidad alta que afectan a Cups Easy, un software de compras e inventario basado en PHP, las cuales han sido descubiertas por Rafael Pedrero.

A estas vulnerabilidades se le han asignado los siguientes códigos, con misma puntuación base CVSS v3.1, vector del CVSS y el tipo de vulnerabilidad CWE:

CVE-2024-23855 al CVE-2024-23896: 7.1 | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:N | CWE-79.

## Avisos técnicos - Hasta el 8 de febrero

# Vulnerabilidades de severidad alta en Google Chrome

Google ha emitido un aviso de seguridad actualizando el canal estable 121.0.6167.85 para Mac y Linux y 121.0.6167.85/.86 para Windows, que se lanzará en los próximos días/semanas, donde se corrigen 11 vulnerabilidades, de las cuales 3 son categorizadas con severidad alta con los identificadores CVE-2024-0807, CVE-2024-0812, CVE-2024-0808.

Avisos técnicos - Hasta el 8 de febrero

# Vulnerabilidades en Mozilla Firefox, ESR y Thunderbird

Mozilla ha emitido avisos de seguridad donde se tratan múltiples vulnerabilidades que afectan al navegador Firefox, Firefox ERS y al cliente de correo electrónico multiplataforma Mozilla Thunderbird.

Dentro de estas, destacan 5 de severidad alta cuyos identificadores son CVE-2024-0741, CVE-2024-0742, CVE-2024-0743, CVE-2024-0744 y CVE-2024-0745, que, de ser explotadas, pueden resultar en condiciones de desbordamiento de búfer basado en la pila y escritura fuera de límites, entre otros.

Avisos técnicos - Hasta el 8 de febrero

# Vulnerabilidad zero-day en productos Apple

Apple ha publicado varios avisos de seguridad, donde se trata una vulnerabilidad zero-day que afecta al componente Webkit en el navegador Safari y los sistemas operativos iOS, iPadOS, macOS Sonoma, mac OS Ventura, macOs Monterey y tvOS, cuyo identificador es CVE-2024-23222, que, de ser explotada, conduce a condiciones de ejecución de código arbitrario.

Avisos técnicos - Hasta el 8 de febrero

# Ejecución remota de código en productos de Cisco

Cisco ha publicado una vulnerabilidad de severidad crítica que podría permitir al atacante ejecutar comandos arbitrarios en el sistema operativo subyacente con los privilegios del usuario de servicios web. En caso de tener acceso al sistema operativo subyacente, el atacante también podría establecer acceso root en el dispositivo afectado.

Avisos técnicos - Hasta el 8 de febrero

# Vulnerabilidad crítica en productos Cisco Unified Communications

Cisco ha publicado un aviso de seguridad para tratar una vulnerabilidad, de severidad critica, que afecta a varios productos de soluciones de comunicaciones unificadas y centros de contacto de Cisco. El identificador de este error, que podría permitir al atacante ejecutar comandos arbitrarios en el sistema operativo subyacente con los privilegios del usuario de servicios web, así como establecer acceso de root en el dispositivo afectado, es el CVE-2024-20253.

Avisos técnicos - Hasta el 8 de febrero

# Vulnerabilidad Cross-Site Scripting en IceHrm

INCIBE ha coordinado la publicación de una vulnerabilidad de severidad media, que afecta a IceHrm versión 23.0.0.OS, un sistema de gestión de recursos humanos, la cual ha sido descubierta por Rafael Pedrero.

A esta vulnerabilidad se le ha asignado el siguiente código, puntuación base CVSS v3.1, vector del CVSS y el tipo de vulnerabilidad CWE:

CVE-2023-6282: 5.4 | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N | CWE-79.

Avisos técnicos - Hasta el 8 de febrero

# Lectura arbitraria de archivos en Jenkins

Jenkins ha publicado una vulnerabilidad de severidad crítica en su informe de seguridad, la cual afecta al núcleo de sistema y su explotación podría provocar una ejecución remota de código.

Avisos técnicos - Hasta el 8 de febrero

# Vulnerabilidad en productos NAS de Zyxel

Zyxel ha publicado un aviso de seguridad sobre una nueva vulnerabilidad de severidad alta con el identificador CVE-2023-5372. Esta vulnerabilidad de inyección de comando posterior a la autenticación afecta a algunas versiones de sus productos NAS.

Avisos técnicos - Hasta el 8 de febrero

# Vulnerabilidad de desbordamiento de búfer en Resource Hacker

INCIBE ha coordinado la publicación de 1 vulnerabilidad de severidad alta que afecta a Resource Hacker versión 3.6.0.92, un editor de recursos para aplicaciones Windows de 32 y 64 bits desarrollado por Angus Johnson, la cual ha sido descubierta por Rafael Pedrero.

Avisos técnicos - Hasta el 8 de febrero

# Vulnerabilidades de alta severidad en Google Chrome

Google ha emitido un aviso de seguridad actualizando el canal estable 121.0.6167.139 para Mac y Linux y 121.0.6167.139/140 para Windows, que se lanzará en los próximos días/semanas, donde se corrigen 4 vulnerabilidades, de las cuales 3 son categorizadas con severidad alta con los identificadores CVE-2024-1060, CVE-2024-1059, CVE-2024-1077.

Avisos técnicos - Hasta el 8 de febrero

# Actualización de seguridad de Apple-Enero 2024

A lo largo de enero, Apple ha publicado 10 actualizaciones de seguridad en las que se corrigen 30 vulnerabilidades que afectan a los sistemas operativos iOS, iPadOS, macOS Sonoma, macOS Ventura, macOS Monterey, tvOS, watchOS, y al navegador Safari.

Entre las múltiples vulnerabilidades reportadas, las más graves, de ser explotadas, pueden conducir a condiciones de ejecución de código arbitrario, denegación de servicio, acceso a la información confidencial del usuario, y divulgación de datos de la memoria del kernel, entre otros.

## Avisos técnicos - Hasta el 8 de febrero

# Múltiples vulnerabilidades en la librería glibc de distribuciones Linux

El equipo Qualys Threat Research Unit (TRU) ha descubierto 4 vulnerabilidades en la librería GNU C (glibc), concretamente en las funciones syslog y qsort. Un atacante sin privilegios podría obtener acceso root en varias de las principales distribuciones de Linux, en configuraciones predeterminadas, mediante una escalada de privilegios local.

Avisos técnicos - Hasta el 8 de febrero

# Vulnerabilidades de alta severidad en productos de Ivanti

Ivanti ha publicado un aviso de seguridad para tratar dos vulnerabilidades de severidad alta, CVE-2024-21888 de escalada de privilegios y CVE-2024-21893 de Server-Side Request Forgery (SSRF). Estos errores afectan a los productos Ivanti Policy Secure Gateways, Ivanti Connect Secure e Ivanti Neurons for ZTA, que, de ser explotados, podrían suponer una amenaza de gravedad crítica para varios productos de Ivanti con un impacto en la confidencialidad de los sistemas que se vean afectados.

Avisos técnicos - Hasta el 8 de febrero

# Múltiples vulnerabilidades en JSA de Juniper

Júniper ha publicado un informe de 20 vulnerabilidades de diferentes severidades, destacando 2 de ellas de severidad crítica.

## Avisos técnicos - Hasta el 8 de febrero

# Vulnerabilidad de ruta de búsqueda o elemento no entrecomillado en HDD Health de PanteraSoft

INCIBE ha coordinado la publicación de una vulnerabilidad de severidad alta que afecta a HDD Health, una herramienta de monitorización de discos duros desarrollada por PanteraSoft, la cual ha sido descubierta por Jorge Manuel Lozano Gómez.

Avisos técnicos - Hasta el 8 de febrero

# Leaky Vessels: múltiples vulnerabilidades en componentes de contenedores

Rory McNamara, investigador de Synk, junto con el equipo Snyk Security Labs, han reportado 4 vulnerabilidades que han recibido el apodo de Leaky Vessels. Estas 4 vulnerabilidades, 2 de severidad crítica y 2 altas, se han detectado en componentes centrales de la infraestructura de contenedores que podrían permitir escapes de contenedores. Un atacante podría utilizar estos escapes de contenedores para obtener acceso no autorizado al sistema operativo host subyacente desde el interior del contenedor.

Avisos técnicos - Hasta el 8 de febrero

# Vulnerabilidades en productos de Qnap

Qnap ha emitido varios avisos de seguridad para tratar vulnerabilidades en los productos QTS, QuTS hero, QuTScloud, y Qsync Central. Dentro de ellos, los de más relevancia son los que están categorizados con una severidad alta que cuenta con los identificadores CVE-2023-45025, CVE-2023-39297, CVE-2023-47564, CVE-2023-47567 y CVE-2023-47568. Estos fallos, de ser explotados, pueden tener un impacto grave en la confidencialidad, disponibilidad e integridad de los sistemas.

Avisos técnicos - Hasta el 8 de febrero

# Incidente de seguridad en AnyDesk

AnyDesk ha activado un plan de reparación y respuesta, en el que ha participado la compañía de ciberseguridad Crowdstrike, tomando las medidas correspondientes tales como reemplazar los sistemas comprometidos y asegurar la integridad de la versión más reciente del software.

Avisos técnicos - Hasta el 8 de febrero

# Múltiples vulnerabilidades en Http File Server de Rejetto

INCIBE ha coordinado la publicación de 2 vulnerabilidades de severidades alta y media respectivamente, que afectan a Rejetto Http File Server (HFS), versión 2.2a build #124, las cuales han sido descubiertas por Rafael Pedrero.

Avisos técnicos - Hasta el 8 de febrero

# IMúltiples vulnerabilidades en HPE UOCAM

HPE Product Security Response Team ha reportado 17 vulnerabilidades en el producto Unified OSS Console Assurance Monitoring (UOCAM). Estas vulnerabilidades se clasifican en 7 de severidad crítica, 5 altas 4 medias y 1 baja. Estas vulnerabilidades podrían explotarse para permitir la ejecución remota de código arbitrario, la denegación de servicio, la ejecución local de código arbitrario y la modificación arbitraria de archivos.

Avisos técnicos - Hasta el 8 de febrero

# Boletín de seguridad de Android: febrero de 2024

El boletín de Android, relativo a febrero de 2024, soluciona múltiples vulnerabilidades de severidad crítica y alta que afectan a su sistema operativo, así como múltiples componentes, que podrían provocar una escalada de privilegios, una divulgación de información o una ejecución remota de código.

## Avisos técnicos - Hasta el 8 de febrero

# Actualización de seguridad de Android-Febrero 2024

Google ha publicado las actualizaciones de seguridad de Android y dispositivos Píxel del mes de febrero de 2024, en donde se corrigen 53 vulnerabilidades, que abarcan soluciones para fallos de elevación de privilegios, divulgación de información y ejecución remota de código.

Avisos técnicos - Hasta el 8 de febrero

# Vulnerabilidades de severidad alta en Google Chrome

Google ha emitido un aviso de seguridad actualizando el canal estable 121.0.6167.160 para Mac y Linux y 121.0.6167.160/161 para Windows, que se lanzará en los próximos días/semanas, donde se corrigen 2 vulnerabilidades, de severidad alta con los identificadores CVE-2024-1284 y CVE-2024-1283.

Avisos técnicos - Hasta el 8 de febrero

# Múltiples vulnerabilidades en FortiSIEM de Fortinet

El investigador, Zach Hanley (@hacks_zach), de Horizon3.ai, ha reportado 3 vulnerabilidades críticas que afectan al producto FortiSIEM de Fortinet. La explotación de estas vulnerabilidades podría permitir a un atacante remoto, no autenticado, ejecutar comandos no autorizados a través de solicitudes de API falsificadas.

Avisos técnicos - Hasta el 8 de febrero

# Omisión de autenticación mediante una ruta o canal alternativo en TeamCity de JetBrains

JetBrains ha publicado una vulnerabilidad de severidad crítica que podría permitir a un atacante, no autenticado, con acceso HTTP(S) a un servidor TeamCity, eludir las comprobaciones de autenticación y obtener control administrativo.

Avisos técnicos - Hasta el 8 de febrero

# Vulnerabilidad XSS en productos Liferay

Liferay ha publicado un aviso para informar de una vulnerabilidad crítica de tipo Cross-Site Scripting (XSS) que afecta a varios productos.

Avisos técnicos - Hasta el 8 de febrero

# Lectura arbitraria de archivos en Jenkins

Jenkins ha publicado una vulnerabilidad de severidad crítica en su informe de seguridad, la cual afecta al núcleo de sistema y su explotación podría provocar una ejecución remota de código.

Avisos técnicos - Hasta el 8 de febrero

# Vulnerabilidad en productos NAS de Zyxel

Zyxel ha publicado un aviso de seguridad sobre una nueva vulnerabilidad de severidad alta con el identificador CVE-2023-5372. Esta vulnerabilidad de inyección de comando posterior a la autenticación afecta a algunas versiones de sus productos NAS.

Avisos técnicos - Hasta el 8 de febrero

# Vulnerabilidad de desbordamiento de búfer en Resource Hacker

INCIBE ha coordinado la publicación de 1 vulnerabilidad de severidad alta que afecta a Resource Hacker versión 3.6.0.92, un editor de recursos para aplicaciones Windows de 32 y 64 bits desarrollado por Angus Johnson, la cual ha sido descubierta por Rafael Pedrero.

Avisos técnicos - Hasta el 8 de febrero

# Vulnerabilidades de alta severidad en Google Chrome

Google ha emitido un aviso de seguridad actualizando el canal estable 121.0.6167.139 para Mac y Linux y 121.0.6167.139/140 para Windows, que se lanzará en los próximos días/semanas, donde se corrigen 4 vulnerabilidades, de las cuales 3 son categorizadas con severidad alta con los identificadores CVE-2024-1060, CVE-2024-1059, CVE-2024-1077.

Avisos técnicos - Hasta el 8 de febrero

# Actualización de seguridad de Apple-Enero 2024

A lo largo de enero, Apple ha publicado 10 actualizaciones de seguridad en las que se corrigen 30 vulnerabilidades que afectan a los sistemas operativos iOS, iPadOS, macOS Sonoma, macOS Ventura, macOS Monterey, tvOS, watchOS, y al navegador Safari.

Entre las múltiples vulnerabilidades reportadas, las más graves, de ser explotadas, pueden conducir a condiciones de ejecución de código arbitrario, denegación de servicio, acceso a la información confidencial del usuario, y divulgación de datos de la memoria del kernel, entre otros.

## Avisos técnicos - Hasta el 8 de febrero

# Múltiples vulnerabilidades en la librería glibc de distribuciones Linux

El equipo Qualys Threat Research Unit (TRU) ha descubierto 4 vulnerabilidades en la librería GNU C (glibc), concretamente en las funciones syslog y qsort. Un atacante sin privilegios podría obtener acceso root en varias de las principales distribuciones de Linux, en configuraciones predeterminadas, mediante una escalada de privilegios local.

Avisos técnicos - Hasta el 8 de febrero

# Vulnerabilidades de alta severidad en productos de Ivanti

Ivanti ha publicado un aviso de seguridad para tratar dos vulnerabilidades de severidad alta, CVE-2024-21888 de escalada de privilegios y CVE-2024-21893 de Server-Side Request Forgery (SSRF). Estos errores afectan a los productos Ivanti Policy Secure Gateways, Ivanti Connect Secure e Ivanti Neurons for ZTA, que, de ser explotados, podrían suponer una amenaza de gravedad crítica para varios productos de Ivanti con un impacto en la confidencialidad de los sistemas que se vean afectados.

Avisos técnicos - Hasta el 8 de febrero

# Múltiples vulnerabilidades en JSA de Juniper

Júniper ha publicado un informe de 20 vulnerabilidades de diferentes severidades, destacando 2 de ellas de severidad crítica.

## Avisos técnicos - Hasta el 8 de febrero

# Vulnerabilidad de ruta de búsqueda o elemento no entrecomillado en HDD Health de PanteraSoft

INCIBE ha coordinado la publicación de una vulnerabilidad de severidad alta que afecta a HDD Health, una herramienta de monitorización de discos duros desarrollada por PanteraSoft, la cual ha sido descubierta por Jorge Manuel Lozano Gómez.

Avisos técnicos - Hasta el 8 de febrero

# Leaky Vessels: múltiples vulnerabilidades en componentes de contenedores

Rory McNamara, investigador de Synk, junto con el equipo Snyk Security Labs, han reportado 4 vulnerabilidades que han recibido el apodo de Leaky Vessels. Estas 4 vulnerabilidades, 2 de severidad crítica y 2 altas, se han detectado en componentes centrales de la infraestructura de contenedores que podrían permitir escapes de contenedores. Un atacante podría utilizar estos escapes de contenedores para obtener acceso no autorizado al sistema operativo host subyacente desde el interior del contenedor.

Avisos técnicos - Hasta el 8 de febrero

# Vulnerabilidades en productos de Qnap

Qnap ha emitido varios avisos de seguridad para tratar vulnerabilidades en los productos QTS, QuTS hero, QuTScloud, y Qsync Central. Dentro de ellos, los de más relevancia son los que están categorizados con una severidad alta que cuenta con los identificadores CVE-2023-45025, CVE-2023-39297, CVE-2023-47564, CVE-2023-47567 y CVE-2023-47568. Estos fallos, de ser explotados, pueden tener un impacto grave en la confidencialidad, disponibilidad e integridad de los sistemas.

Avisos técnicos - Hasta el 8 de febrero

# Incidente de seguridad en AnyDesk

AnyDesk ha activado un plan de reparación y respuesta, en el que ha participado la compañía de ciberseguridad Crowdstrike, tomando las medidas correspondientes tales como reemplazar los sistemas comprometidos y asegurar la integridad de la versión más reciente del software.

Avisos técnicos - Hasta el 8 de febrero

# Múltiples vulnerabilidades en Http File Server de Rejetto

INCIBE ha coordinado la publicación de 2 vulnerabilidades de severidades alta y media respectivamente, que afectan a Rejetto Http File Server (HFS), versión 2.2a build #124, las cuales han sido descubiertas por Rafael Pedrero.

Avisos técnicos - Hasta el 8 de febrero

# IMúltiples vulnerabilidades en HPE UOCAM

HPE Product Security Response Team ha reportado 17 vulnerabilidades en el producto Unified OSS Console Assurance Monitoring (UOCAM). Estas vulnerabilidades se clasifican en 7 de severidad crítica, 5 altas 4 medias y 1 baja. Estas vulnerabilidades podrían explotarse para permitir la ejecución remota de código arbitrario, la denegación de servicio, la ejecución local de código arbitrario y la modificación arbitraria de archivos.

Avisos técnicos - Hasta el 8 de febrero

# Boletín de seguridad de Android: febrero de 2024

El boletín de Android, relativo a febrero de 2024, soluciona múltiples vulnerabilidades de severidad crítica y alta que afectan a su sistema operativo, así como múltiples componentes, que podrían provocar una escalada de privilegios, una divulgación de información o una ejecución remota de código.

## Avisos técnicos - Hasta el 8 de febrero

# Actualización de seguridad de Android-Febrero 2024

Google ha publicado las actualizaciones de seguridad de Android y dispositivos Píxel del mes de febrero de 2024, en donde se corrigen 53 vulnerabilidades, que abarcan soluciones para fallos de elevación de privilegios, divulgación de información y ejecución remota de código.

Avisos técnicos - Hasta el 8 de febrero

# Vulnerabilidades de severidad alta en Google Chrome

Google ha emitido un aviso de seguridad actualizando el canal estable 121.0.6167.160 para Mac y Linux y 121.0.6167.160/161 para Windows, que se lanzará en los próximos días/semanas, donde se corrigen 2 vulnerabilidades, de severidad alta con los identificadores CVE-2024-1284 y CVE-2024-1283.

Avisos técnicos - Hasta el 8 de febrero

# Múltiples vulnerabilidades en FortiSIEM de Fortinet

El investigador, Zach Hanley (@hacks_zach), de Horizon3.ai, ha reportado 3 vulnerabilidades críticas que afectan al producto FortiSIEM de Fortinet. La explotación de estas vulnerabilidades podría permitir a un atacante remoto, no autenticado, ejecutar comandos no autorizados a través de solicitudes de API falsificadas.

Avisos técnicos - Hasta el 8 de febrero

# Omisión de autenticación mediante una ruta o canal alternativo en TeamCity de JetBrains

JetBrains ha publicado una vulnerabilidad de severidad crítica que podría permitir a un atacante, no autenticado, con acceso HTTP(S) a un servidor TeamCity, eludir las comprobaciones de autenticación y obtener control administrativo.

Avisos técnicos - Hasta el 8 de febrero

# Vulnerabilidad XSS en productos Liferay

Liferay ha publicado un aviso para informar de una vulnerabilidad crítica de tipo Cross-Site Scripting (XSS) que afecta a varios productos.

Avisos técnicos - Hasta el 8 de febrero

# Múltiples vulnerabilidades en la serie Cisco Expressway

Cisco ha publicado 3 vulnerabilidades: 2 de severidad crítica y 1 alta que podrían permitir que un atacante remoto, no autenticado, realice ataques de falsificación de solicitudes entre sitios (CSRF) y acciones arbitrarias en un dispositivo afectado.

Avisos técnicos - Hasta el 8 de febrero

# Vulnerabilidades críticas en Cisco Expressway Series

Cisco ha publicado un aviso de seguridad para tratar vulnerabilidades de severidad critica en Cisco Expressway Series. Los identificadores de estos errores, de falsificación de solicitudes entre sitios, son CVE-2024-20252, CVE-2024-20254, CVE-2024-20255.

Avisos técnicos - Hasta el 8 de febrero

# Múltiples vulnerabilidades en LaborOfficeFree

INCIBE ha coordinado la publicación de 4 vulnerabilidades de severidad media que afectan a LaborOfficeFree versión 19.10, las cuales han sido descubiertas por Pedro Gabaldón Juliá, Javier Medina Munuera, Antonio José Gálvez Sánchez y Alejandro Baño Andrés.

Avisos técnicos - Hasta el 8 de febrero