

Hasta el 8 de junio

# AVISOS TÉCNICOS



# Subida de ficheros no controlada en TIBCO EBX Add-ons

---

TIBCO ha notificado una vulnerabilidad de severidad crítica que podría permitir a un atacante subir archivos a un directorio accesible por el servidor web.

Avisos técnicos - Hasta el 8 de junio

# Inyección SQL en Jorani

---

INCIBE ha coordinado la publicación de 1 vulnerabilidad que afecta a Jorani, la cual ha sido descubierta por David Utón Amaya (m3n0sd0n4ld).

A esta vulnerabilidad se le ha asignado el código CVE-2023-2681.

Se ha calculado una puntuación base CVSS v3.1 de 8,8, siendo el cálculo del CVSS el siguiente: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H.

Avisos técnicos - Hasta el 8 de junio

# Vulnerabilidad en dispositivos NAS de Zyxel

---

Zyxel ha publicado un aviso de seguridad en la que se corrige una vulnerabilidad que afecta a algunos dispositivos de almacenamiento conectados en red (NAS). Los modelos en cuestión son Zyxel NAS326, NAS540 y NAS542. El error, de severidad alta, cuenta con el identificador CVE-2023-27988 y podría producir una condición de inyección de comandos del sistema operativo de forma remota. Su explotación implica un alto impacto en la confidencialidad, integridad y disponibilidad de los sistemas.

Avisos técnicos - Hasta el 8 de junio



# Múltiples vulnerabilidades en BuddyBoss

---

INCIBE ha coordinado la publicación de 3 vulnerabilidades en la plataforma BuddyBoss, que han sido descubiertas por Anxo Januario Gonzales.

Avisos técnicos - Hasta el 8 de junio

# Actualización de seguridad de Joomla! 4.3.2

---

Los investigadores Srpopty y Phil Taylor han reportado al JSST (Joomla! Security Strike Team) 2 vulnerabilidades que afectan al core de Joomla! CMS.

Avisos técnicos - Hasta el 8 de junio

# Vulnerabilidades en Google Chrome

---

Google ha hecho público un aviso de seguridad donde se trata la actualización de Google Chrome a la versión 114, dentro del canal estable, que se encuentra disponible para su descarga y uso general. En el aviso se han resuelto un total de 16 errores, teniendo 8 una severidad calificada como alta por parte de la compañía y cuyos identificadores son CVE-2023-2929, CVE-2023-2930, CVE-2023-2931, CVE-2023-2932, CVE-2023-2933, CVE-2023-2934, CVE-2023-2935, CVE-2023-2936.

Avisos técnicos - Hasta el 8 de junio

# Múltiples vulnerabilidades en NXLog Manager

---

INCIBE ha coordinado la publicación de 3 vulnerabilidades en NXLog Manager, una consola de gestión y supervisión de agentes, que han sido descubiertas por Juampa Rodríguez.

Avisos técnicos - Hasta el 8 de junio



# Vulnerabilidad de bypass de autorización en UPV PEIX

---

INCIBE ha coordinado la publicación de una vulnerabilidad en UPV PEIX, un sistema de gestión de prácticas de empresa de la Escuela Técnica Superior de Ingeniería Informática de la Universitat Politècnica de València (UPC), que ha sido descubierta por Pablo Alcarria Lozano y Germán Planells García.

Avisos técnicos - Hasta el 8 de junio

# Actualización de seguridad de Apple-Mayo 2023

---

A lo largo del mes de mayo, Apple ha publicado 11 actualizaciones de seguridad en las que se corrigen 61 fallos que afectan a iTunes para Windows, al navegador Safari, a los sistemas operativos iOS, macOS Ventura, macOS Monterey, macOS Big Sur, watchOS, iPadOS y tvOS, y por último a los auriculares Powerbeats para los que se ofrece una actualización de firmware. Entre las múltiples vulnerabilidades reportadas, las más graves son las que podrían permitir la ejecución de código arbitrario, de forma que, un atacante podría explotar algunas de ellas para tomar el control de un dispositivo afectado.

Avisos técnicos - Hasta el 8 de junio

# Vulnerabilidad de inyección SQL en MOVEit Transfer de Progress

---

Progress ha informado sobre una vulnerabilidad crítica de inyección SQL detectada en su producto MOVEit Transfer, cuya explotación podría permitir a un atacante no autenticado acceder a la base de datos de dicho producto.

Avisos técnicos - Hasta el 8 de junio



# Vulnerabilidades críticas en firewalls ZyWall de Zyxel

---

Zyxel ha publicado una guía que proporciona orientación y recomendaciones sobre cómo abordar y mitigar los problemas relacionados con los recientes ataques a dispositivos ZyWall. Las vulnerabilidades que los atacantes están utilizando son CVE-2023-28771, CVE-2023-33009 y CVE-2023-33010. La explotación de estas vulnerabilidades puede llevar a la ejecución remota de código y la denegación de servicio, lo que representa una amenaza significativa para la confidencialidad, integridad y disponibilidad de los sistemas afectados.

Avisos técnicos - Hasta el 8 de junio



# Actualización de seguridad de Android-Junio 2023

---

Google ha publicado las actualizaciones de seguridad para Android del mes de junio de 2023 en donde se corrigen 56 vulnerabilidades de las versiones 10, 11, 12 y 13 del sistema operativo y componentes asociados, abarcando soluciones para fallos de denegación de servicio, elevación de privilegios, divulgación de información y ejecución remota de código. De todas ellas, 5 están calificadas con una severidad crítica y 51 altas.

Avisos técnicos - Hasta el 8 de junio

# Vulnerabilidades en Firefox

---

Mozilla ha emitido un aviso de seguridad que aborda cinco vulnerabilidades, siendo tres de ellas de gravedad alta. Estas vulnerabilidades se identifican como CVE-2023-34414, CVE-2023-34416 y CVE-2023-34417, y su explotación puede resultar en la ejecución remota de código y suplantación de identidad.

Avisos técnicos - Hasta el 8 de junio

# Vulnerabilidades críticas en VMware Aria Operations

---

VMware ha publicado un aviso de seguridad que aborda tres vulnerabilidades identificadas como CVE-2023-20887, CVE-2023-20888, ambas de severidad crítica y CVE-2023-20889 de severidad alta. La explotación de las vulnerabilidades críticas podría permitir a los atacantes realizar inyecciones remotas de código, mientras que la de severidad alta podría resultar en la divulgación de información. Todas estas vulnerabilidades representan una amenaza grave para la confidencialidad, disponibilidad e integridad de los sistemas.

Avisos técnicos - Hasta el 8 de junio



# Múltiples vulnerabilidades en VMware Aria Operations Networks

---

El investigador, Sina Kheirkhah, de Summoning Team, en colaboración con ZDI de Trend Micro, han reportado 3 vulnerabilidades, 2 de severidad crítica y 1 alta, cuya explotación podría permitir a un atacante ejecutar código remoto o divulgar información.

Avisos técnicos - Hasta el 8 de junio



# Vulnerabilidades en productos de Cisco

---

Cisco, compañía relacionada con el sector de redes y tecnología, ha publicado un total de siete avisos de seguridad, donde se destaca una vulnerabilidad calificada con una severidad crítica y cuatro errores que cuentan con una puntuación alta. Dichos errores afectan a Cisco Expressway Series, Cisco TelePresence, Cisco Unified Communications Manager IM and Presence Service, Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software for Firepower 2100 Series Appliances SSL/TLS, Cisco AnyConnect Secure Mobility Client Software para Windows y Cisco Secure Client Software para Windows.

Avisos técnicos - Hasta el 8 de junio