Del 12 al 25 de mayo

AVISOS TÉCNICOS

EUSKO JAURLARITZA
GOBIERNO VASCO
EKONOMIAREN GARAPEN, JASANGARRITASUN ETA INGURUMEN SAILA
DEPARTAMENTO DE DESARROLLO ECONÓMICO, SOSTENIBILIDAD Y MEDIO AMBIENTE

GRUPO spri TALDEA

Basque CyberSecurity Centre

Vulnerabilidades en VMware Aria Operations

VMware ha publicado un aviso de seguridad que aborda cuatro vulnerabilidades identificadas como CVE-2023-20877, CVE-2023-20878, CVE-2023-20879, CVE-2023-20880. La primera de estas vulnerabilidades es un fallo de escalada de privilegios de alta gravedad, lo que la convierte en la más relevante dentro de la actualización. Su explotación podría tener un impacto significativo en la confidencialidad, integridad y disponibilidad de los sistemas afectados. Las vulnerabilidades restantes cuentan una severidad moderada.

Avisos técnicos - Del 12 al 25 de mayo

Vulnerabilidad crítica en plugin de WordPress

Wordfence, un equipo compuesto por analistas de seguridad de WordPress, ha lanzado un anuncio de seguridad en el que se destaca una vulnerabilidad que ha sido catalogada con una severidad crítica. Dicho fallo afecta al plugin Essential Addons for Elementor, que cuenta con más de un millón de descargas.

Avisos técnicos - Del 12 al 25 de mayo

Vulnerabilidades en Google ChromeOS

Google ha hecho público un aviso de seguridad, anunciando una actualización del canal de asistencia para ChromeOS. El aviso del canal de asistencia para ChormeOS, contiene un total de 3 errores, que han sido todos ellos calificados con una severidad alta y registrados con los identificadores CVE-2023-2135, CVE-2023-2134, CVE-2023-2133. La explotación de todos estos fallos supondría un impacto de alta gravedad en la disponibilidad, integridad y confidencialidad de los sistemas afectados.

Avisos técnicos - Del 12 al 25 de mayo

Vulnerabilidades críticas en Apache

Apache ha actualizado el estado de dos avisos de seguridad, aviso para Apache Airflow y aviso para Apache bPRC, que hacen referencia a dos vulnerabilidades de severidad crítica para los productos Apache Airflow y Apache bRPC. Los identificadores de estos fallos son CVE-2023-25754 y CVE-2023-31039 respectivamente. Su explotación exitosa, en ambos casos, supone un impacto de alta gravedad en la confidencialidad, integridad y disponibilidad de los sistemas afectados.

Avisos técnicos - Del 12 al 25 de mayo

Actualización de seguridad 6.2.1 para WordPress

Se ha publicado la última versión de WordPress que contiene correcciones de seguridad.

Avisos técnicos - Del 12 al 25 de mayo

Actualización de seguridad 6.2.2 para WordPress

Se ha publicado la última versión de WordPress que contiene correcciones de seguridad.

Avisos técnicos - Del 12 al 25 de mayo

Vulnerabilidad crítica en Django

Se ha actualizado el estado de una vulnerabilidad publicada en un aviso de seguridad el pasado 3 de mayo de 2023 que afecta al framework de desarrollo web Django. La vulnerabilidad, cuyo identificador es CVE-2023-31047, es un fallo crítico de bypass en la validación de formularios y cuya explotación exitosa supondría un alto impacto sobre la confidencialidad, integridad y disponibilidad de los sistemas afectados.

Avisos técnicos - Del 12 al 25 de mayo

Vulnerabilidades en Switches Cisco Small Business Series

Cisco ha publicado un aviso de seguridad donde se tratan 9 vulnerabilidades que afectan a algunos Switches de la gama Cisco Small Business Series. Los identificadores de las vulnerabilidades con una severidad crítica son CVE-2023-20159, CVE-2023-20160, CVE-2023-20161, CVE-2023-20189 y la explotación de todas ellas supone una alta gravedad para la confidencialidad, disponibilidad e integridad de los sistemas afectados.

Avisos técnicos - Del 12 al 25 de mayo

Vulnerabilidad Oday en Mikrotik RouterOS

Angelboy(@scwuaptx) y NiNi (@terrynini38514), investigadores de DEVCORE Research Team, han reportado una vulnerabilidad 0day en Mikrotik RouterOS RADVD, cuya explotación podría permitir a un atacante ejecutar código arbitrario con privilegios de root.

Avisos técnicos - Del 12 al 25 de mayo

Vulnerabilidades zero-day en Apple

Apple ha publicado diversos avisos de seguridad, en los que se abordan tres vulnerabilidades de tipo zero-day que se deben a errores existentes en el componente WebKit, afectando a sistemas iOS, iPadOS, macOS Ventura, macOS Monterey, macOS Big Sur, watchOS y tvOS. Las vulnerabilidades, identificadas bajo los CVE-2023-32409, CVE-2023-28204 y CVE-2023-32373, de momento no tienen asignadas una puntuación de acuerdo a la escala CVSSv3, pero han sido calificadas por el fabricante como de tipo zero-day, por lo tanto se les asigna una severidad crítica.

Avisos técnicos - Del 12 al 25 de mayo

Múltiples vulnerabilidades en Junos Space de Juniper Networks

Se han corregido 17 vulnerabilidades detectadas durante una investigación de seguridad. 2 de ellas de severidad crítica, 7 de severidad alta y el resto medias y bajas.

Avisos técnicos - Del 12 al 25 de mayo

Vulnerabilidad de lectura arbitraria de archivos en GitLab

El investigador pwnie ha informado de una vulnerabilidad de severidad crítica que podría permitir la lectura arbitraria de archivos en el servidor.

Avisos técnicos - Del 12 al 25 de mayo

Vulnerabilidad crítica en GitLab

GitLab ha publicado una actualización de seguridad en la que se aborda una vulnerabilidad, cuya severidad ha sido calificada como crítica, y que afecta a la aplicación de código abierto utilizada para alojar repositorios Git, conocida como GitLab Community Edition (CE). De igual manera, GitLab Enterprise Edition (EE), una plataforma de programación dirigida al desarrollo y ejecución software de aplicaciones escritas en Java, es vulnerable ante el error destacado.

Avisos técnicos - Del 12 al 25 de mayo

Vulnerabilidad en PowerVM Hypervisor de IBM

IBM informa de una vulnerabilidad de severidad crítica que podría provocar la fuga de datos o la ejecución de código arbitrario en otras particiones lógicas en el mismo servidor.

Avisos técnicos - Del 12 al 25 de mayo

Vulnerabilidades críticas en productos de Zyxel

Zyxel ha emitido un aviso de seguridad que aborda dos vulnerabilidades críticas para algunos productos de seguridad de red que están siendo afectados por errores de desbordamiento de búfer. Estos fallos cuentan con los identificadores CVE-2023-33009 y CVE-2023-33010 y pueden conducir a condiciones de denegación de servicio y ejecución remota de código. Su explotación exitosa tiene un impacto significativo en la confidencialidad, integridad y disponibilidad de los sistemas afectados.

Avisos técnicos - Del 12 al 25 de mayo