Hasta el 4 de enero

AVISOS TÉCNICOS

EUSKO JAURLARITZA
GOBIERNO VASCO

cyber zaintza

Múltiples vulnerabilidades en productos de Dell EMC

Dell ha informado de varias vulnerabilidades en sus productos Dell EMC Avamar Server y Dell EMC Integrated Data Protection Appliance (IDPA) que podrían comprometer completamente la aplicación vulnerable y el sistema operativo subyacente, así como la eliminación de datos y archivos arbitrarios.

Avisos técnicos - Hasta el 4 de enero

Actualización de seguridad dispositivos Google Pixel-Diciembre 2023

Google ha publicado las actualizaciones de seguridad para los dispositivos Google Pixel del mes de diciembre de 2023, en donde se corrigen 33 vulnerabilidades abarcando soluciones para fallos de denegación de servicio, elevación de privilegios, divulgación de información y ejecución remota de código. De todas ellas, 3 están calificadas con una severidad crítica, 6 alta y 24 moderada.

Avisos técnicos - Hasta el 4 de enero

Múltiples vulnerabilidades en productos de Atlassian

Atlassian ha informado en varios avisos de seguridad sobre vulnerabilidades críticas que afectan a productos de Confluence, Jira, Companion y Assets Discovery. La explotación de estas vulnerabilidades podría conducir a la ejecución remota de código.

Avisos técnicos - Hasta el 4 de enero

Cross-Site Request Forgery en OPEN JOURNAL SYSTEMS

INCIBE ha coordinado la publicación de una vulnerabilidad que afecta a OJS (OPEN JOURNAL SYSTEMS), una solución de código abierto para la gestión y publicación de revistas académicas en línea, en su versión 3.3.0.13, la cual ha sido descubierta por David Cámara Galindo, de Telefónica Tech.

Avisos técnicos - Hasta el 4 de enero

Boletín de seguridad de Android: diciembre de 2023

El boletín de Android, relativo a diciembre de 2023, 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, divulgación de información, denegación de servicio o conducir a la ejecución remota de código.

Avisos técnicos - Hasta el 4 de enero

Múltiples vulnerabilidades en Repox

INCIBE ha coordinado la publicación de 6 vulnerabilidades que afectan a Repox 2.3.7, un marco para administrar espacios de datos, las cuales han sido descubiertas por David Cámara Galindo y Andrés Elizalde Galdeano, de Telefónica Tech.

Avisos técnicos - Hasta el 4 de enero

Múltiples vulnerabilidades en productos de Apple

Apple ha informado sobre varias vulnerabilidades, algunas de tipo 0day, que podrían permitir a un atacante ejecutar código arbitrario.

Avisos técnicos - Hasta el 4 de enero

Actualización de seguridad de SAP-Diciembre 2023

SAP ha publicado las actualizaciones de seguridad correspondientes al mes de diciembre para una amplia gama de sus productos. En total, se han notificado 15 nuevas notas de seguridad, a las que se añaden 2 actualizaciones de notas publicadas con anterioridad. De todas ellas, 4 se clasifican con una severidad crítica, 4 con una severidad alta, 7 media y 2 baja, corrigiendo fallos de divulgación de información, falta de autorización, control de acceso inadecuado y falsificación de solicitudes.

Avisos técnicos - Hasta el 4 de enero

Actualización de seguridad de Microsoft-Diciembre 2023

Microsoft ha publicado las actualizaciones de seguridad del mes de diciembre de 2023 en las que se corrigen 37 vulnerabilidades, siendo 4 de ellas calificadas como críticas, 30 como importantes, 1 moderada, 2 bajas y 5 sin un valor asignado que afectan al navegador Edge basado en Chromium.

Avisos técnicos - Hasta el 4 de enero

Múltiples vulnerabilidades en HPE vTeMIP

HPE Product Security Response Team ha notificado múltiples vulnerabilidades, de severidades crítica, alta y media, que afectan a HPE vTeMIP, cuya explotación podría permitir a un atacante corromper la memoria, desbordar la pila de memoria y realizar una denegación de servicio (DoS).

Avisos técnicos - Hasta el 4 de enero

Control de acceso inadecuado en FortiMail de Fortinet

El equipo de investigadores de FortiGuard Labs ha reportado una vulnerabilidad crítica que afecta a la solución de seguridad de correo electrónico FortiMail, cuya explotación podría permitir a un atacante omitir el proceso de autenticación.

Avisos técnicos - Hasta el 4 de enero

Actualización de seguridad de SAP de diciembre de 2023

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

Avisos técnicos - Hasta el 4 de enero

Vulnerabilidades de alto impacto en productos de Fortinet

Fortinet ha publicado varios avisos de seguridad para tratar 1 vulnerabilidad de severidad crítica, con el identificador CVE-2023-47539, que afecta al producto FortiMail.

Avisos técnicos - Hasta el 4 de enero

Actualizaciones de seguridad de Microsoft de diciembre de 2023

La publicación de actualizaciones de seguridad de Microsoft, correspondiente a la publicación de vulnerabilidades del 12 de diciembre, consta de 36 vulnerabilidades (con CVE asignado), calificadas 2 como críticas, 23 como importantes y como 11 medias.

Avisos técnicos - Hasta el 4 de enero

Múltiples vulnerabilidades en Amazing Little Poll

INCIBE ha coordinado la publicación de 2 vulnerabilidades que afectan a Amazing Little Poll, un script en PHP para la generación de encuestas, las cuales han sido descubiertas por David Utón Amaya (m3n0sd0n4ld).

Avisos técnicos - Hasta el 4 de enero

Vulnerabilidad crítica en Apache Struts con impacto en productos Cisco

Cisco ha publicado un aviso de seguridad para tratar una vulnerabilidad, de severidad critica, en Apache Struts, divulgada públicamente por la Apache Software Foundation el pasado 7 de diciembre de 2023. El identificador de este error, que puede posibilitar la manipulación de los parámetros de carga de archivos y conducir a la ejecución de código remoto, es el CVE-2023-50164.

Avisos técnicos - Hasta el 4 de enero

Vulnerabilidades en Google Chrome

Google ha publicado un aviso de seguridad actualizando el canal estable para Windows, Mac y Linux, donde se corrigen 5 vulnerabilidades de severidad alta cuyos identificadores son CVE-2023-6702, CVE-2023-6703, CVE-2023-6704, CVE-2023-6705 y CVE-2023-6706.

Avisos técnicos - Hasta el 4 de enero

Vulnerabilidades 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 Jira Software Data Center y Server, Confluence Data Server, Crowd Data Center y Server, Bitbucket Data Center y Server y Bamboo Data Center y Server.

Avisos técnicos - Hasta el 4 de enero

Múltiples vulnerabilidades en HPE Intelligent Management Center

HPE Product Security Response Team ha reportado múltiples vulnerabilidades que afectan a su producto Intelligent Management Center, cuya explotación podría permitir a un atacante ejecutar código, realizar una denegación de servicio (DoS) o acceder a datos no autorizados.

Avisos técnicos - Hasta el 4 de enero

Vulnerabilidad de escalada de privilegios en Intel Driver & Support Assistant

Se ha reportado una vulnerabilidad 0day de severidad alta en productos Intel, cuya explotación podría permitir a un atacante remoto realizar una escalada de privilegios.

Avisos técnicos - Hasta el 4 de enero

Vulnerabilidad en PAN OS de Palo Alto Networks

Palo Alto ha publicado un aviso de seguridad para corregir 1 vulnerabilidad de severidad alta que afecta al software PAN OS, y que conduce a una condición de Cross Site Scripting (XSS), cuyo identificador es CVE-2023-6790. Este error, de ser explotado, supondría una amenaza de alta gravedad para la confidencialidad, integridad y disponibilidad de los sistemas.

Avisos técnicos - Hasta el 4 de enero

Secuestro de sesión en Imou Life app

INCIBE ha coordinado la publicación de 1 vulnerabilidad de secuestro de sesión que afecta a Imou Life app 6.7.0, la cual ha sido descubierta por Jan Adamski (johnny1337.pl).

Avisos técnicos - Hasta el 4 de enero

XML External Entity Reference en 52North WPS

INCIBE ha coordinado la publicación de 1 vulnerabilidad que afecta a 52North WPS en versiones hasta 4.0.0-beta.11, la cual ha sido descubierta por Ángel Heredia Pérez.

Avisos técnicos - Hasta el 4 de enero

Múltiples vulnerabilidades en OpenSSH

Se ha publicado la versión 9.6 de OpenSSH, que contiene una serie de correcciones de seguridad, destacando 3 vulnerabilidades descubiertas por los investigadores Fabian Bäumer, Marcus Brinkmann y Jörg Schwenk, de la Universidad Ruhr de Bochum, y que se ha denominado Terrapin Attack. La explotación de estas vulnerabilidades podría permitir un ataque MitM que rompiese la integridad del canal seguro de SSH.

Avisos técnicos - Hasta el 4 de enero

Múltiples vulnerabilidades en Ivanti

Ivanti ha publicado 3 vulnerabilidades de severidad alta con un factor de riesgo crítico que podrían provocar un desbordamiento de búfer.

Avisos técnicos - Hasta el 4 de enero

Vulnerabilidades en productos de Zimbra

Zimbra ha publicado varios avisos de seguridad donde se tratan vulnerabilidades de severidad alta aprovechando un ataque de inyección de código mediante Javascript. Las vulnerabilidades abordadas tienen los identificadores CVE-2023-21930, CVE-2022-21476, CVE-2022-21449 y CVE-2023-48432.

Avisos técnicos - Hasta el 4 de enero

Vulnerabilidades en Mozilla Firefox 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.

Avisos técnicos - Hasta el 4 de enero

Vulnerabilidad 0-day en Google Chrome

Google ha emitido un aviso de seguridad actualizando el canal estable para Windows, Mac y Linux, donde se corrige 1 vulnerabilidad 0-day de la que se conoce que existe un exploit. El identificador asociado a este fallo es el CVE-2023-7024 y afecta al componente webRTC, dando lugar a una condición de desbordamiento del buffer del Heap si se produce la explotación de la misma.

Avisos técnicos - Hasta el 4 de enero

Múltiples vulnerabilidades en Unified OSS Console de HPE

El equipo de respuesta de seguridad de productos de HPE ha informado que, una vulnerabilidad de severidad crítica y dos vulnerabilidades de severidad alta ya reportadas, afectan a uno de sus productos. La explotación de estas vulnerabilidades podría permitir a un atacante remoto evadir las restricciones de acceso, realizar una ejecución arbitraria de código, evadir la autenticación, comprometer la integridad del sistema, y desbordar el búfer.

Avisos técnicos - Hasta el 4 de enero

Comunicación del servidor no autenticada en D-Link D-View 8

El equipo de investigación de Tenable ha publicado una vulnerabilidad crítica que afecta al software de administración de red D-View 8 del fabricante D-Link.

Avisos técnicos - Hasta el 4 de enero

Múltiples vulnerabilidades en Juniper Secure Analytics

Se han reportado 18 vulnerabilidades en Juniper Secure Analytics, de las cuales: 2 son de severidad baja, 7 de severidad media, 7 de severidad alta, y 2 de severidad crítica.

Avisos técnicos - Hasta el 4 de enero

Actualización de seguridad de Apple-Diciembre 2023

A lo largo de diciembre, Apple ha publicado 12 actualizaciones de seguridad en las que se corrigen 44 vulnerabilidades que afectan a los sistemas operativos iOS, iPadOS, macOS Sonoma, macOS Ventura, macOS Monterey, tvOS, watchOS, y al navegador Safari.

Avisos técnicos - Hasta el 4 de enero

Boletín de seguridad de Android: enero de 2024

El boletín de Android, relativo a enero 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 o una divulgación de información.

Avisos técnicos - Hasta el 4 de enero