Del 14 al 26 de abril

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

Múltiples vulnerabilidades en HP Device Manager

HP ha informado de 31 vulnerabilidades en su producto Device Manager, 5 de ellas de severidad crítica, cuya explotación podría permitir inyectar comandos y/o escalar privilegios.

Avisos técnicos - Del 14 al 26 de abril

Vulnerabilidades en Cisco IOS y IOS XE

Cisco ha publicado la actualización de un aviso de seguridad donde se tratan múltiples vulnerabilidades de severidad alta, cuyos identificadores son CVE-2017-6736, CVE-2017-6737, CVE-2017-6738, CVE-2017-6739, CVE-2017-6740, CVE-2017-6741, CVE-2017-6742, CVE-2017-6743, CVE-2017-6744, que afectan al protocolo SNMP (Simple Network Management Protocol) en los sistemas operativos Cisco IOS y IOS XE.

Avisos técnicos - Del 14 al 26 de abril

Vulnerabilidades en Google Chrome

Google ha publicado una actualización de seguridad para el navegador Chrome que aborda varias vulnerabilidades identificadas como CVE-2023-1529, CVE-2023-1528, CVE-2023-1533, CVE-2023-1534, CVE-2023-1530. La explotación exitosa de estas vulnerabilidades podría tener un impacto significativo en la confidencialidad, integridad y disponibilidad de los sistemas afectados.

Avisos técnicos - Del 14 al 26 de abril

Actualizaciones críticas en Oracle (abril 2023)

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

Avisos técnicos - Del 14 al 26 de abril

Múltiples vulnerabilidades en Control de Ciber

INCIBE ha coordinado la publicación de 3 vulnerabilidades en el aplicativo Control de Ciber, que han sido descubiertas por Sergio Apellániz.

A estas vulnerabilidades se les han asignado los códigos: CVE-2022-4896, CVE-2022-48474 y CVE-2022-48475.

Para las 3 vulnerabilidades, se ha calculado una puntuación base CVSS v3.1 de 7,3, siendo el cálculo del CVSS el siguiente: AV:N/AC:L/PR:N/UI:N/S:U/C:L/N:N/A:H.

Avisos técnicos - Del 14 al 26 de abril

Subida de archivos sin restricciones en TIBCO Spotfire

Se ha identificado una vulnerabilidad crítica en TIBCO Spotfire que permite la subida de ficheros sin restricciones.

Avisos técnicos - Del 14 al 26 de abril

Omisión de acceso en el core de Drupal

La explotación de esta vulnerabilidad podría dar lugar a que los usuarios obtengan acceso a archivos privados a los que no deberían tenerlo.

Avisos técnicos - Del 14 al 26 de abril

Vulnerabilidades en sistemas y productos de Cisco

Cisco ha publicado varios avisos de seguridad, cisco-sa-ind-CAeLFk6V, cisco-sa-cml-auth-bypass-4fUCCeG5, cisco-sa-staros-ssh-privesc-BmWeJC3h, cisco-sa-bw-tcp-dos-KEdJCxLs en los que se abordan vulnerabilidades de severidad crítica, alta y media. Los identificadores de los fallos tratados son CVE-2023-20036, CVE-2023-20039, CVE-2023-20154, CVE-2023-20046, CVE-2023-20125. Por otra parte, se ha actualizado el aviso cisco-sa-20170629-snmp reportado con anterioridad.

Avisos técnicos - Del 14 al 26 de abril

Últimas vulnerabilidades en Google Chrome

Google ha hecho público un aviso de seguridad, anunciando una actualización del escritorio en canal estable para Google Chrome, en donde se han resuelto un total de 8 errores, teniendo 4 vulnerabilidades una severidad calificada como alta por parte de la compañía.

Avisos técnicos - Del 14 al 26 de abril

Vulnerabilidad en el Core de Drupal

Drupal ha publicado un aviso de seguridad, sa-core-2023-005, donde se trata una vulnerabilidad de severidad alta que afecta a la función de descarga de archivos que en ciertas circunstancias permite que los usuarios accedan a archivos privados a los que no deberían tener acceso. Este fallo, de ser explotado, produce un impacto moderado en la confidencialidad de los sistemas afectados.

Avisos técnicos - Del 14 al 26 de abril

Actualización de seguridad de Oracle-Abril 2023

El 18 de abril de 2023 Oracle publicó su boletín trimestral de actualizaciones de seguridad en el que se aportan 433 correcciones a vulnerabilidades para una amplia gama de productos. Algunas de estas vulnerabilidades pueden ser explotadas por un atacante remoto para comprometer la integridad, confidencialidad y disponibilidad de los sistemas afectados, lo que podría resultar en una pérdida de datos y una interrupción de los servicios.

Avisos técnicos - Del 14 al 26 de abril

Múltiples vulnerabilidades en VMware Aria Operations for Logs

Diversos investigadores han reportado 2 vulnerabilidades, 1 crítica y 1 alta, que afectan Aria Operations for Logs de VMware, cuya explotación podría permitir a un atacante ejecutar código/comandos arbitrarios como root.

Avisos técnicos - Del 14 al 26 de abril

Vulnerabilidades de impacto crítico en VMware

VMWare ha publicado un aviso de seguridad donde se tratan 2 vulnerabilidades, CVE-2023-20864, CVE-2023-20865, de severidades crítica y alta respectivamente, que afectan al producto VMware Aria Operations for Logs. Ambos fallos, de ser explotados, permitirían a un atacante ejecutar código arbitrario en los sistemas afectados produciendo un alto impacto en la confidencialidad, integridad y disponibilidad de los mismos.

Avisos técnicos - Del 14 al 26 de abril

Vulnerabilidades en VMware Workstation y VMware Fusion

VMWare ha publicado un aviso de seguridad donde se tratan 4 vulnerabilidades cuyos identificadores son CVE-2023-20869, CVE-2023-20870, CVE-2023-20871, CVE-2023-20872, siendo la primera de severidad crítica y el resto alta, que afectan a los productos VMware Workstation y VMware Fusion. La explotación de estos fallos puede conducir a condiciones de ejecución de código, escalada de privilegios y lectura fuera de los límites, propiciando todas ellas un alto impacto en la confidencialidad de los sistemas afectados.

Vulnerabilidades en PrestaShop

Prestashop ha publicado un 3 avisos de seguridad, GHSA-p379-cxqh-q822, GHSA-8r4m-5p6p-52rp y GHSA-fh7r-996q-gvcp donde se tratan 3 vulnerabilidades cuyos identificadores son CVE-2023-30839, CVE-2023-30545 y CVE-2023-30838, siendo la primera de severidad crítica y las dos restantes de severidad alta. La explotación de estos fallos puede conducir a condiciones de omisión del filtro SQL, lectura de archivos arbitrarios y de inyección XSS (Cross-Site-Scripting), propiciando, en el caso de los fallos de más gravedad, un alto impacto en la confidencialidad, integridad y disponibilidad de los sistemas afectados.

Avisos técnicos - Del 14 al 26 de abril