Hasta el 11 de octubre

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 módulos de Drupal

Drupal ha publicado dos avisos de seguridad, sa-contrib-2023-046, donde se corrige una vulnerabilidad crítica que afecta al módulo Entity cache y sa-contrib-2023-047, en el que se trata una vulnerabilidad de severidad alta en el módulo Content Moderation Notifications. La explotación del error crítico supone un impacto de alta gravedad en la confidencialidad e integridad de los sistemas afectados.

Avisos técnicos - Hasta el 11 de octubre

Múltiples vulnerabilidades en productos Exim

ZDI ha publicado 4 vulnerabilidades: 3 de severidad alta y una de severidad crítica la cual, permite a atacantes remotos ejecutar código arbitrario en las instalaciones afectadas de Exim.

Avisos técnicos - Hasta el 11 de octubre

[Actualización 02/10/2023] Múltiples vulnerabilidades en productos Exim

ZDI ha publicado 4 vulnerabilidades: 3 de severidad alta y una de severidad crítica la cual, permite a atacantes remotos ejecutar código arbitrario en las instalaciones afectadas de Exim.

Avisos técnicos - Hasta el 11 de octubre

[Actualización 03/10/2023] Múltiples vulnerabilidades en productos Exim

ZDI ha publicado 4 vulnerabilidades: 3 de severidad alta y una de severidad crítica la cual, permite a atacantes remotos ejecutar código arbitrario en las instalaciones afectadas de Exim.

Avisos técnicos - Hasta el 11 de octubre

Vulnerabilidades en Google Chrome y ChromeOS

Google ha publicado dos avisos de seguridad actualizando el canal estable para Windows, Mac y Linux y el canal de soporte a largo plazo (LTS) para ChromeOS. En ellos se corrigen 7 vulnerabilidades de severidad alta cuyos identificadores son CVE-2023-5217, CVE-2023-5186, CVE-2023-5187, CVE-2023-4863, CVE-2023-4429, CVE-2023-4572, CVE-2023-4428. Cabe destacar que desde Google se advierte que el fallo CVE-2023-5217 puede estar siendo explotado.

Avisos técnicos - Hasta el 11 de octubre

Vulnerabilidades de alto impacto en productos Cisco

Cisco, compañía relacionada con el sector de redes y tecnología, ha publicado un total de dieciséis avisos de seguridad donde se destacan cinco vulnerabilidades catalogadas con una severidad crítica, y un total de siete vulnerabilidades calificadas con una criticidad alta. Dichos errores afectan a Cisco SD-WAN, Cisco IOS XE y Cisco DNA Center.

Avisos técnicos - Hasta el 11 de octubre

Vulnerabilidad en la librería libwebp para imágenes WebP

Se ha identificado una vulnerabilidad crítica 0day en la librería libwebp. Mediante la creación y el envío a potenciales víctimas de imágenes WebP maliciosas, los atacantes podrían aprovechar esta vulnerabilidad para ejecutar código arbitrario y acceder a datos confidenciales del usuario.

Avisos técnicos - Hasta el 11 de octubre

Múltiples vulnerabilidades en WS_FTP Server de Progress

Shubham Shah y Sean Yeoh, de Assetnote, y Cristian Mocanu, de Deloitte, han reportado 8 vulnerabilidades, de las cuales 2 son de severidad crítica, 3 de severidad alta, y de 3 severidad media.

La explotación de estas vulnerabilidades podría permitir a un atacante ejecutar comandos de forma remota, realizar modificaciones de ficheros y ejecutar código en los recursos afectados.

Avisos técnicos - Hasta el 11 de octubre

Actualización de seguridad de Apple-Septiembre 2023

A lo largo de septiembre, Apple ha publicado 22 actualizaciones de seguridad en las que se corrigen 85 fallos que afectan a los sistemas operativos iOS, iPadOS, macOS Sonoma, macOS Ventura, macOS Monterey, macOS Big Sur, tvOS, watchOS, al navegador Safari y al entorno de desarrollo XCode.

Avisos técnicos - Hasta el 11 de octubre

Boletín de seguridad de Android de octubre de 2023

El boletín de Android, relativo a octubre de 2023, soluciona múltiples vulnerabilidades de severidad crítica y alta que afectan a su sistema operativo, así como múltiples componentes, que podrían permitir a un atacante realizar una escalada de privilegios, divulgar información, provocar una denegación de servicio (DoS) o ejecutar código remoto (RCE).

Avisos técnicos - Hasta el 11 de octubre

Desbordamiento de búfer en librería glibc de distribuciones Linux

Qualys Threat Research Unit (TRU) ha descubierto una vulnerabilidad de severidad alta, denominada Looney Tunables, de tipo desbordamiento de búfer, que afecta a la librería glibc, nombre común utilizado para GNU C Library. La explotación de esta vulnerabilidad podría permitir una escalada local de privilegios que otorgase privilegios completos de root.

Avisos técnicos - Hasta el 11 de octubre

[Actualización 09/10/2023] Desbordamiento de búfer en librería glibc de distribuciones Linux

Qualys Threat Research Unit (TRU) ha descubierto una vulnerabilidad de severidad alta, denominada Looney Tunables, de tipo desbordamiento de búfer, que afecta a la librería glibc, nombre común utilizado para GNU C Library. La explotación de esta vulnerabilidad podría permitir una escalada local de privilegios que otorgase privilegios completos de root.

Avisos técnicos - Hasta el 11 de octubre

Vulnerabilidad zero-day en productos Apple

Apple ha publicado un aviso de seguridad en el que se aborda una nueva vulnerabilidad zero-day, cuyo identificador es CVE-2023-42824, que afecta al kernel de los sistemas operativos iOS 17.0.3 y iPadOS 17.0.3, y que, de ser explotada, conduce a una condición de escalada de privilegios. Desde Apple se afirma tener conocimiento de un informe que indica que este problema puede haber sido explotado activamente en versiones de iOS anteriores a iOS 16.6.

Avisos técnicos - Hasta el 11 de octubre

Actualización de seguridad de Android-Octubre 2023

Google ha publicado las actualizaciones de seguridad de Android y los dispositivos Google Pixel del mes de octubre de 2023, en donde se corrigen 51 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 46 alta. En cuanto a los dispositivos Google Pixel, se corrigen 28 vulnerabilidades, con 2 de severidad crítica, 5 altas y 21 moderadas.

Avisos técnicos - Hasta el 11 de octubre

Vulnerabilidad crítica en Confluence Data Center y Server de Atlassian

Atlassian ha publicado un aviso de seguridad donde se trata 1 vulnerabilidad crítica de escalada de privilegios en Confluence Data Center y Confluence Server, cuyo identificador es CVE-2023-22515. Desde Atlassian se informa que este fallo, previamente desconocido, puede estar siendo explotado por atacantes externos para crear cuentas de administrador de Confluence no autorizadas y acceder a instancias de Confluence, lo que supone una amenaza de alta gravedad para la confidencialidad, integridad y disponibilidad de los sistemas afectados.

Avisos técnicos - Hasta el 11 de octubre

Últimas vulnerabilidades en productos Cisco

Cisco, compañía relacionada con el sector de redes y tecnología, ha publicado un total de cuatro avisos de seguridad donde se destaca una vulnerabilidad catalogada con una severidad crítica, y un total de dos vulnerabilidades calificadas con una criticidad alta. Dichos errores afectan a Cisco Emergency Responder, Cisco Network Services Orchestrator y Cisco Unified Communications.

Avisos técnicos - Hasta el 11 de octubre

Vulnerabilidades en Sophos Firewall y Sophos UTM

Sophos ha emitido un aviso de seguridad que aborda múltiples vulnerabilidades divulgadas con impacto en los productos Sophos Firewall y Sophos UTM. Estas vulnerabilidades están relacionadas con el software de correo Exim, un agente de transferencia de mensajes de código abierto. Entre las vulnerabilidades más relevantes se encuentran CVE-2023-42115, clasificada como crítica y CVE-2023-42116, CVE-2023-42117, CVE-2023-42118, que tienen una gravedad alta. La explotación de todas ellas conduce a la ejecución remota de código.

Avisos técnicos - Hasta el 11 de octubre

Control de acceso roto en el Confluence Data Center y Server de Atlassian

La vulnerabilidad de severidad crítica notifacada es debida a un acceso público para crear cuentas de administrador de Confluence, no autorizadas, y acceder a sus instancias.

Avisos técnicos - Hasta el 11 de octubre

Múltiples vulnerabilidades en D-View de D-Link

rgod ha notificado varias vulnerabilidades 0day, entre ellas dos de severidad crítica, que podrían permitir a atacantes remotos eludir la autenticación o ejecutar código arbitrario.

Avisos técnicos - Hasta el 11 de octubre

Actualización de seguridad de SAP-Octubre 2023

SAP ha publicado las actualizaciones de seguridad correspondientes al mes de octubre para una amplia gama de sus productos. En total, se han notificado 7 nuevas notas de seguridad, a las que se añaden 2 actualizaciones de notas publicadas con anterioridad. De todas ellas, 1 se clasifica como de severidad crítica y 8 media, corrigiendo fallos de divulgación de información, falsificación de solicitudes, Cross-Site Scripting (XSS) e inyección de registros, entre otros.

Avisos técnicos - Hasta el 11 de octubre