Del 3 al 16 de marzo

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

Vulnerabilidad de alta severidad en Cisco APIC

Cisco ha publicado un aviso de seguridad donde se aportan soluciones a un fallo de alto impacto en las aplicaciones Cisco Application Policy Infrastructure Controller y Cisco Cloud Network Controller. La vulnerabilidad cuyo identificador es CVE-2023-20011, podría permitir que un atacante remoto no autenticado realizase un ataque de falsificación de solicitud entre sitios (CSRF), lo que conllevaría un alto impacto en la confidencialidad, integridad y disponibilidad del sistema afectado.

Avisos técnicos - Del 3 al 16 de marzo

Vulnerabilidad crítica en Qnap QTS y QuTS hero

Qnap ha publicado un aviso de seguridad donde se corrige una vulnerabilidad crítica, cuyo identificador es CVE-2022-27596. El fallo afecta a los dispositivos QNAP que ejecutan QTS 5.0.1 y QuTS hero h5.0.1 y, de ser explotado, podría permitir a los atacantes, de forma remota, inyectar código malintencionado lo que conlleva un alto impacto en la confidencialidad, integridad y disponibilidad de los sistemas afectados.

Avisos técnicos - Del 3 al 16 de marzo

Múltiples vulnerabilidades en Aspera Faspex de IBM

IBM ha publicado 10 vulnerabilidades en su boletín de seguridad de las cuales 1 es de severidad crítica, que podría permitir a un atacante ejecutar código de forma remota; 3 de severidad alta y 6 de severidad media.

Avisos técnicos - Del 3 al 16 de marzo

Boletín de seguridad de Android de marzo de 2023

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

Avisos técnicos - Del 3 al 16 de marzo

Múltiples vulnerabilidades en productos de Fortinet

Fortinet ha publicado varios avisos de seguridad, FG-IR-23-001, FG-IR-22-281, FG-IR-22-309, FG-IR-22-401, FG-IR-23-050 y FG-IR-22-254, en donde se trata, en el primero de ellos, una vulnerabilidad crítica con el identificador CVE-2023-25610, en FortiOS y FortiProxy. En los restantes se corrigen fallos de severidad alta que afectan a los productos FortiNAC, ForiSOAR, FortiWeb y también a FortiOS y FortiProxy. Los identificadores son CVE-2022-39953, CVE-2022-42476, CVE-2023-25605, CVE-2022-39951 y CVE-2022-40676.

Avisos técnicos - Del 3 al 16 de marzo

Actualización de seguridad de Android – Marzo 2023

Google ha publicado las actualizaciones de seguridad para Android del mes de marzo de 2023 donde se corrigen 55 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 las 55 vulnerabilidades tratadas, 4 tienen una severidad crítica, y 51 alta.

Avisos técnicos - Del 3 al 16 de marzo

Vulnerabilidad de alta severidad en enrutadores Cisco ASR 9000

Cisco ha hecho público un nuevo aviso de seguridad donde se corrige una vulnerabilidad de severidad alta que afecta al software Cisco IOS XR para enrutadores Cisco ASR 9000 Series Aggregation Services Routers, ASR 9902 Compact High-Performance Routers y ASR 9903 Compact High-Performance Routers. El identificador de este fallo es CVE-2023-20049 que tras una explotación exitosa, puede conducir a una condición de denegación de servicio afectando a la disponibilidad de los sistemas afectados.

Avisos técnicos - Del 3 al 16 de marzo

Actualización de seguridad de SAP – Marzo 2023

SAP ha publicado las actualizaciones de seguridad correspondientes al mes de marzo para una amplia gama de sus productos. En total, se han notificado 19 nuevas notas de seguridad de las cuales 5 se clasifican como críticas, 4 altas y 10 como medias, corrigiendo fallos de ejecución remota de código, denegación de servicio, inyección de entidad externa XML (XXE), Cross-Site Scripting (XSS) y divulgación de información, entre otras.

Avisos técnicos - Del 3 al 16 de marzo

Actualizaciones de seguridad de Microsoft de marzo de 2023

La publicación de actualizaciones de seguridad de Microsoft, correspondiente al mes de marzo y que incluye toda la información comprendida entre los días 15/02/2023 y 14/03/2023, consta de 109 vulnerabilidades (con CVE asignado), calificadas como: 9 de severidad crítica, 70 importantes, 1 moderada y 29 sin severidad asignada.

Avisos técnicos - Del 3 al 16 de marzo

Múltiples vulnerabilidades en productos ClearPass Policy Manager de Aruba

Aruba ha publicado actualizaciones para solucionar 7 vulnerabilidades de seguridad (una de ellas crítica) que podrían provocar divulgación de información confidencial, escalada de privilegios, omisión de autenticación, Cross-Site Scripting (XSS), divulgación de información confidencial y obtener acceso no autorizado.

Avisos técnicos - Del 3 al 16 de marzo

Actualización de seguridad de SAP de marzo de 2023

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

Avisos técnicos - Del 3 al 16 de marzo

Actualización de seguridad de Microsoft marzo 2023

Microsoft ha publicado las actualizaciones de seguridad del mes de marzo de 2023 en las que se corrigen 104 vulnerabilidades, siendo 9 de ellas calificadas como críticas, 70 como importantes, 1 moderada y 24 sin un valor asignado que incluyen, por una parte, al navegador Edge basado en Chromium y a la distribución de Linux CBL-Mariner por otra.

Avisos técnicos - Del 3 al 16 de marzo

Vulnerabilidades en Aruba ClearPass Policy Manager

Aruba, compañía relacionada con diversas soluciones de seguridad, ha publicado un aviso que contiene un total de 8 vulnerabilidades. Entre ellas, se destaca 1 vulnerabilidad que ha sido calificada como crítica por parte del fabricante, además de contar con un total de 4 fallos a los que se les ha asignado una severidad alta.

Avisos técnicos - Del 3 al 16 de marzo

Vulnerabilidades en el Core y módulos de Drupal

Drupal ha publicado 5 actualizaciones de seguridad, sa-contrib-2023-011, sa-contrib-2023-010, sa-core-2023-004, sa-core-2023-003 y sa-core-2023-002 para abordar la corrección de fallos que afectan a varios productos. El primero de ellos, de severidad crítica, afecta al proyecto Responsive media Image Formatter y no está resuelto ya que el proyecto no tiene mantenimiento por parte de sus responsables. El resto, que afectan al core de Drupal y al módulo Media Responsive Thumbnail son de severidad alta y pueden conducir a condiciones de divulgación de información y bypass de acceso.

Avisos técnicos - Del 3 al 16 de marzo