Hasta el 11 de marzo

AVISOS TÉCNICOS

EUSKO JAURLARITZA
GOBIERNO VASCO

cyber zaintza

Ejecución remota de código en Azure de Microsoft

Nitesh Surana (@_niteshsurana) de Trend Micro Research, ha notificado una vulnerabilidad de severidad crítica que podría permitir a un atacante remoto ejecutar código arbitrario.

Avisos técnicos - Hasta el 11 de marzo

Vulnerabilidad Server-Side Request Forgery en productos de Haivision

INCIBE ha coordinado la publicación de una vulnerabilidad de severidad media que afecta a Aviwest Manager y Aviwest Streamhub de Haivision, dos herramientas de monitorización de vídeo y gestión de dispositivos, la cual ha sido descubierta por Konrad Kowal Karp de Telefónica Tech.

Avisos técnicos - Hasta el 11 de marzo

Vulnerabilidades en ClearPass Policy Manager de Aruba

Aruba network ha publicado un aviso de seguridad corrigiendo múltiples vulnerabilidades que afectan al producto Clearpass Policy Manager, plataforma de políticas de acceso, la cual proporciona control en la red en base a roles y a dispositivos.

Avisos técnicos - Hasta el 11 de marzo

Vulnerabilidad de Cross-Site Scripting en Cockpit CMS

INCIBE ha coordinado la publicación de una vulnerabilidad de severidad media que afecta a Cockpit CMS versión 2.7.0, un sistema de gestión de contenido autónomo simple y ligero creado para pequeñas y medianas empresas, la cual ha sido descubierta por Sergio Román Hurtado.

Avisos técnicos - Hasta el 11 de marzo

Múltiples vulnerabilidades en Secure Analytics de Juniper

Juniper ha publicado 14 vulnerabilidades de las cuales 2 de ellas son de severidad crítica y el resto altas y medias.

Avisos técnicos - Hasta el 11 de marzo

Vulnerabilidades en Cisco NX-OS

Cisco ha publicado avisos de seguridad para tratar 2 vulnerabilidades, de severidad alta, que afectan al producto Cisco NX-OS, el sistema operativo de centro de datos del fabricante, con los identificadores CVE-2024-20321 y CVE-2024-20267. Estas vulnerabilidades suponen una amenaza de alta gravedad para productos de Cisco con impacto en la disponibilidad de los sistemas que se vean afectados.

Avisos técnicos - Hasta el 11 de marzo

Vulnerabilidad de Cross-Site Scripting en HelpDeskZ

INCIBE ha coordinado la publicación de 1 vulnerabilidad de severidad media que afecta a HelpDeskZ versión 2.0.2 y anteriores, un software basado en PHP que permite la gestión del sitio web a través de asignación de tickets, la cual ha sido descubierta por David Cámara Galindo.

Avisos técnicos - Hasta el 11 de marzo

Boletín de seguridad de Android: marzo de 2024

El boletín de Android, relativo a marzo de 2024, soluciona múltiples vulnerabilidades de severidad crítica y alta que afectan a su sistema operativo, así como múltiples componentes, que podrían provocar la ejecución remota de código sin necesidad de privilegios de ejecución adicionales.

Avisos técnicos - Hasta el 11 de marzo

Vulnerabilidad en Mozilla Thunderbird

Mozilla ha emitido un nuevo aviso de seguridad donde se trata una vulnerabilidad que afectan al cliente de correo electrónico multiplataforma Mozilla Thunderbird. La vulnerabilidad está considerada con una criticidad alta y cuenta con el identificador el CVE-2024-1936. El error produce el filtrado de asuntos de correos electrónicos cifrados a otras conversaciones, ya que el cifrado PGP puede cambiar el asunto de un correo, si selecciona otro, mientras el primero se está descifrando.

Avisos técnicos - Hasta el 11 de marzo

Múltiples vulnerabilidades en JetBrains TeamCity On-Premises

Stephen Fewer, investigador de seguridad de Rapid7, descubrió en febrero de 2024 dos vulnerabilidades, una de severidad crítica y otra alta, que reportó al fabricante JetBrains. Ambas vulnerabilidades son de tipo omisión de autenticación.

Avisos técnicos - Hasta el 11 de marzo

[Actualización 08/03/2024] Múltiples vulnerabilidades en JetBrains TeamCity On-Premises

Stephen Fewer, investigador de seguridad de Rapid7, descubrió en febrero de 2024 dos vulnerabilidades, una de severidad crítica y otra alta, que reportó al fabricante JetBrains. Ambas vulnerabilidades son de tipo omisión de autenticación.

Avisos técnicos - Hasta el 11 de marzo

Vulnerabilidad de Cross-Site Scripting en TP-Link Archer AX50

INCIBE ha coordinado la publicación de 1 vulnerabilidad de severidad media que afecta a TP-Link Archer AX50 versión 1.0.11 build 2022052, un dispositivo router de doble banda, la cual ha sido descubierta por Víctor Fresco Perales (@hacefresko).

Avisos técnicos - Hasta el 11 de marzo

Actualización de seguridad de Android-Marzo 2024

Google ha publicado las actualizaciones de seguridad de Android y dispositivos Píxel del mes de marzo de 2024, en donde se corrigen 92 vulnerabilidades, que abarcan soluciones para fallos de elevación de privilegios, divulgación de información y ejecución remota de código.

Avisos técnicos - Hasta el 11 de marzo

Vulnerabilidad de Cross-Site Scripting en Gophish Admin Panel

NCIBE ha coordinado la publicación de una vulnerabilidad de severidad media que afecta a Gophish Admin Panel versión 0.12.1, framework de código abierto para crear plataformas de phishing y comprobar la exposición de la organización, la cual ha sido descubierta por Miguel Segovia Gil.

Avisos técnicos - Hasta el 11 de marzo

Vulnerabilidades críticas en VMware ESXi, Workstation y Fusion

VMware ha publicado un aviso de seguridad relativo a 4 vulnerabilidades de severidad crítica, con los identificadores CVE-2024-22252, CVE-2024-22253, CVE-2024-22254, CVE-2024-22255, que afectan a los productos VMware ESXi, Workstation y Fusion. Estos errores producen condiciones Use-After-Free, escritura fuera de límites y de divulgación de información, suponiendo, las de más severidad, una amenaza de alta gravedad con impacto en la confidencialidad, integridad y disponibilidad de los sistemas que se vean afectados.

Avisos técnicos - Hasta el 11 de marzo

Vulnerabilidades en ArubaOS

Aruba network ha publicado un aviso de seguridad corrigiendo múltiples vulnerabilidades que afectan a los productos ArubaOS, sistema operativo desarrollado por Aruba Networks y al software SD-WAN, la red de área local definida por software SD-WAN.

Avisos técnicos - Hasta el 11 de marzo

[Actualización 08/03/2024] Múltiples vulnerabilidades 0day en productos de Apple

Apple ha publicado 4 vulnerabilidades, 2 de ellas de tipo 0day, que podrían permitir a un atacante eludir las protecciones de la memoria del kernel.

Avisos técnicos - Hasta el 11 de marzo

Vulnerabilidades en Google Chrome

Google ha publicado avisos de seguridad donde, por una parte, se actualiza el canal LTS para ChromeOS, donde se corrigen 2 vulnerabilidades de severidad alta cuyos identificadores son CVE-2024-0225 y CVE-2024-1059. Estas vulnerabilidades producen condiciones Use-After-Free en el software WebGPU y WebRTC.

Avisos técnicos - Hasta el 11 de marzo

Vulnerabilidades zero-day en iOS y iPadOS de Apple

Apple ha publicado avisos de seguridad, donde se tratan 2 vulnerabilidades zero-day que afectan al Kernel de iOS y iPadOS, y al componente RTKit. Los identificadores de estas vulnerabilidades son CVE-2024-23225 y CVE-2024-23296 y conducen a una condición de corrupción de la memoria.

Avisos técnicos - Hasta el 11 de marzo

Vulnerabilidad de Cross-Site Scripting en moziloCMS

INCIBE ha coordinado la publicación de una vulnerabilidad de severidad media que afecta a moziloCMS versión 2.0, sistema de gestión de contenidos (CMS) sencillo y fácil de usar para usuarios con pocos conocimientos de HTML, la cual ha sido descubierta por Juampa Rodríguez.

Avisos técnicos - Hasta el 11 de marzo

Vulnerabilidades en Cisco Secure Client

Cisco ha publicado avisos de seguridad para tratar 2 vulnerabilidades de severidad alta en Cisco Secure Client. Los identificadores de estas vulnerabilidades son CVE-2024-20338, CVE-2024-20337. Su explotación supone una amenaza de alta gravedad para la confidencialidad de los sistemas que se vean afectados.

Avisos técnicos - Hasta el 11 de marzo

Vulnerabilidad Cross-Site Scripting en Django MarkdownX

INCIBE ha coordinado la publicación de una vulnerabilidad de severidad media que afecta a Django MarkdownX, versión 4.0.2, un complemento de Markdown creado para Django, el framework web de alto nivel de Python, la cual ha sido descubierta por Julian J. Menendez, de Hispasec Sistemas.

Avisos técnicos - Hasta el 11 de marzo

Vulnerabilidad de subida de ficheros sin restricción en ManageEngine Desktop Central

NCIBE ha coordinado la publicación de una vulnerabilidad de severidad critica que afecta a ManageEngine Desktop Central (ahora conocida como Endpoint Central), una solución de seguridad y gestión de endpoints unificada que ayuda a administrar equipos de escritorio, portátiles, servidores, dispositivos móviles y tablets desde una ubicación central, la cual ha sido descubierta por Rafael Pedrero.

Avisos técnicos - Hasta el 11 de marzo

Actualiza QTS, QuTS hero, QuTScloud y myQNAPcloud para corregir vulnerabilidades

Se han detectado múltiples vulnerabilidades que afectan a algunos sistemas operativos y versiones de aplicaciones de QNAP que, de ser explotadas con éxito, podrían permitir a un ciberdelincuente comprometer la seguridad del sistema, ejecutar comandos e inyectar código malicioso a través de una red.

Avisos técnicos - Hasta el 11 de marzo

Vulnerabilidades en productos QNAP

Qnap ha publicado un aviso de seguridad para tratar 3 vulnerabilidades, 1 de severidad crítica, cuyo identificador es CVE-2024-21899 , así como dos de severidad media cuyos identificadores son CVE-2024-21900 y CVE-2024-21901. Los errores afectan a los productos QTS, QuTS hero, QuTScloud y myQNAPcloud.

Avisos técnicos - Hasta el 11 de marzo