Del 5 al 18 de abril

AVISOS TÉCNICOS

EUSKO JAURLARITZA
GOBIERNO VASCO

cyber zaintza

Múltiples vulnerabilidades en HTTP/2 CONTINUATION Flood

El investigador, Barket Nowotarski, ha reportado múltiples vulnerabilidades que afectan al protocolo HTTP/2 y han recibido el alias de CONTINUATION Flood. La explotación de estas vulnerabilides podría permitir a un atacante ejecutar una denegación de servicio (DoS), bloqueando servidores web con una única conexión TCP en algunas implementaciones.

Avisos técnicos - Del 5 al 18 de abril

Múltiples vulnerabilidades en productos de CData

Un investigador de Tenable ha descubierto 4 vulnerabilidades, 2 de severidad crítica y 2 altas que podrían provocar que un atacante eluda las restricciones de seguridad previstas o realice acciones confidenciales que de otro modo estarían restringidas a un usuario autenticado.

Avisos técnicos - Del 5 al 18 de abril

Ejecución de código remoto en PCOMM de IBM

IBM ha publicado una vulnerabilidad de severidad crítica en su servicio PCOMM que podría permitir a un atacante con pocos privilegios moverse lateralmente a los sistemas afectados y aumentar sus privilegios.

Avisos técnicos - Del 5 al 18 de abril

Actualización de seguridad de SAP-Abril 2024

SAP ha publicado las actualizaciones de seguridad correspondientes al mes de abril para una amplia gama de sus productos. En total, se han notificado 10 nuevas notas de seguridad con 2 actualizaciones de notas publicadas con anterioridad. De todas ellas, 3 se clasifican como severidad alta y 9 como severidad media, corrigiendo fallos de configuración incorrecta, divulgación de información, errores transversales de directorios, denegación de servicio (DDoS), Cross-Site Scripting (XSS) y divulgación de información, entre otros.

Avisos técnicos - Del 5 al 18 de abril

Actualización de seguridad de Microsoft-Abril 2024

Microsoft ha publicado las actualizaciones de seguridad del mes de abril de 2024 en las que se corrigen 157 vulnerabilidades, siendo 3 de ellas calificadas como críticas, 145 como importantes, 3 moderadas, 1 baja y 5 sin un valor asignado que afectan al navegador Edge basado en Chromium.

Estas vulnerabilidades afectan a productos como Microsoft Defender for IoT, Microsoft Office Excel, Azure Private 5G Core, Windows BitLocker, Windows Secure Boot, Microsoft Office Outlook, Windows Kerberos y Azure Migrate, entre otros.

Avisos técnicos - Del 5 al 18 de abril

Actualizaciones de seguridad de Microsoft de abril de 2024

La publicación de actualizaciones de seguridad de Microsoft, correspondiente a la publicación de vulnerabilidades del 9 de abril, consta de 149 vulnerabilidades (con CVE asignado), calificada 1 como crítica que afecta a Microsoft Azure Kubernetes Service, y el resto divididas entre severidades importantes, moderadas y bajas.

Avisos técnicos - Del 5 al 18 de abril

Actualización de seguridad de SAP de abril de 2024

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

Avisos técnicos - Del 5 al 18 de abril

Vulnerabilidades en FortiOS, FortiClientLinux, FortiProxy y FortiSandBox

Fortinet ha publicado varios avisos de seguridad para tratar 1 vulnerabilidad de severidad crítica, cuyo identificador es CVE-2023-45590, que afecta al producto FortiClientLinux, y 6 vulnerabilidades de severidad alta, cuyos identificadores son CVE-2023-45588, CVE-2024-31492, CVE-2023-41677, CVE-2024-23671, CVE-2024-21755 y CVE-2024-21756 que afectan a los productos FortiClientMac installer, FortiProxy y FortiSandbox.

Avisos técnicos - Del 5 al 18 de abril

Múltiples vulnerabilidades en UCA de HPE

HPE ha publicado 11 vulnerabilidades, 5 de severidad crítica y 6 altas que podrían permitir a un atacante ejecución de código, denegación de servicio (DoS), acceso no autorizado, corrupción de memoria, entidad externa XML (XXE) o deserialización insegura.

Avisos técnicos - Del 5 al 18 de abril

Vulnerabilidades en Google Chrome

Google ha publicado un aviso de seguridad actualizando el canal de asistencia a largo plazo para ChromeOS en los sistemas Windows, Mac y Linux, donde se corrigen 3 vulnerabilidades de severidad alta cuyos identificadores son CVE-2024-3157, CVE-2024-3516 y CVE-2024-3515.

Avisos técnicos - Del 5 al 18 de abril

BatBadBut: vulnerabilidad crítica en Rust

RyotaK, investigador de seguridad en Flatt Security, ha reportado una vulnerabilidad de severidad crítica (denominada BatBadBut) al Rust Security Response WG. Un atacante capaz de controlar los argumentos proporcionados al proceso generado podría ejecutar comandos de shell arbitrarios omitiendo el escapado de caracteres.

Avisos técnicos - Del 5 al 18 de abril

Vulnerabilidades en PAN-OS de Palo Alto

Palo Alto ha publicado avisos de seguridad para tratar 4 vulnerabilidades de severidad alta, cuyos identificadores son CVE-2024-3383, CVE-2024-3385, CVE-2024-3382 y CVE-2024-3384, las cuales afectan al producto PAN-OS, el sistema operativo desarrollado por Palo Alto Networks que se utiliza en sus dispositivos de seguridad.

Avisos técnicos - Del 5 al 18 de abril

Vulnerabilidad de ejecución remota de código en JasperReports Server de TIBCO

TIBCO ha reportado una vulnerabilidad de severidad crítica, cuya explotación podría permitir, a un atacante remoto, llevar a cabo una escalada de privilegios, comprometer la red, producir una condición de denegación de servicio, o un ataque de ransomware.

Avisos técnicos - Del 5 al 18 de abril

Múltiples vulnerabilidades en productos LG WebOS

Investigadores de Bitdefender han descubierto 4 vulnerabilidades, 3 de severidad crítica y 1 alta, que afectan al sistema operativo webOS integrado en varios dispositivos Smart TV del fabricante LG. Estas vulnerabilidades podrían permitir a un atacante obtener acceso root en el televisor tras eludir el mecanismo de autorización.

Avisos técnicos - Del 5 al 18 de abril

Vulnerabilidad de Cross-Site Scripting en Teixo de Teimas Global

INCIBE ha coordinado la publicación de una vulnerabilidad de severidad media que afecta a Teixo versión 1.42.42-stable, un software para la gestión de residuos desarrollado por Teimas Global, la cual ha sido descubierta por Iker Loidi Auza.

A esta vulnerabilidad se le ha asignado el siguiente código, puntuación base CVSS v3.1, vector del CVSS y el tipo de vulnerabilidad CWE:

CVE-2024-3654: 6.3 | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L | CWE-79

Avisos técnicos - Del 5 al 18 de abril

Vulnerabilidad de inyección de comandos en Palo Alto Networks PAN-OS

Se ha identificado una vulnerabilidad crítica en PAN-OS, el software que ejecuta todos los firewalls de nueva generación de Palo Alto Networks.

Avisos técnicos - Del 5 al 18 de abril

[Actualización 17/04/2024] Vulnerabilidad de inyección de comandos en Palo Alto Networks PAN-OS

Se ha identificado una vulnerabilidad crítica en PAN-OS, el software que ejecuta todos los firewalls de nueva generación de Palo Alto Networks.

Avisos técnicos - Del 5 al 18 de abril

Múltiples vulnerabilidades en OpenGnsys

INCIBE ha coordinado la publicación de 4 vulnerabilidades: 1 de severidad crítica, 1 de severidad alta, y dos de severidad media, que afectan a OpenGnsys versión 1.1.1d, un conjunto de herramientas libres y abiertas que constituyen un sistema para la gestión y clonación de equipos, las cuales han sido descubiertas por Pedro Gabaldón Julá, Javier Medina Munuera y Antonio José Gálvez Sánchez.

Avisos técnicos - Del 5 al 18 de abril

Vulnerabilidad Crítica en PAN-OS de Palo Alto

Palo Alto ha publicado un aviso de seguridad para tratar 1 vulnerabilidad de severidad crítica, cuyo identificador es CVE-2024-3400, que afecta al producto PAN-OS, el sistema operativo desarrollado por Palo Alto Networks que se utiliza en sus dispositivos de seguridad.

Avisos técnicos - Del 5 al 18 de abril

Exposición de información en CGA2121 de Technicolor

INCIBE ha coordinado la publicación de una vulnerabilidad de severidad alta que afecta al router Technicolor CGA2121 versión 1.01, la cual ha sido descubierta por Edmundo Figueiras Gomez.

A esta vulnerabilidad se le ha asignado el siguiente código, puntuación base CVSS v3.1, vector del CVSS y el tipo de vulnerabilidad CWE:

CVE-2024-3780: 7.8 | CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | CWE-200

Avisos técnicos - Del 5 al 18 de abril

Múltiples vulnerabilidades en WBSAirback de White Bear Solutions

INCIBE ha coordinado la publicación de 16 vulnerabilidades, 1 de severidad crítica, 2 de severidad alta y de 13 de severidad media, que afectan a WBSAirback 21.02.04, las cuales han sido descubiertas por Alejandro Amorín Niño, Guillermo Tuvilla Gómez, Sergio Román Hurtado y Sergio González González (CVE-2024-3781).

Avisos técnicos - Del 5 al 18 de abril

Ejecución de código en productos HPE

HPE ha detectado una vulnerabilidad de severidad crítica que podría llevar a la ejecución de código arbitrario y escalada de privilegios.

Avisos técnicos - Del 5 al 18 de abril

Actualizaciones críticas en Oracle (abril 2024)

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

Avisos técnicos - Del 5 al 18 de abril

Vulnerabilidades de alta severidad 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 Bamboo Data Center y Server, Confluence Data Center y Server, Jira Software Data Center y Server, Jira Service Management Data Center y Server.

Avisos técnicos - Del 5 al 18 de abril

Ejecución remota de código en PCOMM de IBM

IBM ha publicado una vulnerabilidad de severidad crítica que podría provocar una ejecución remota de código (RCE) y escalada de privilegios local (LPE).

Avisos técnicos - Del 5 al 18 de abril

Vulnerabilidades críticas en Ivanti Avalanche

Ivanti ha publicado avisos de seguridad para tratar un total de 28 vulnerabilidades que afectan a Ivanti Avalanche 6.3.1 y versiones superiores, estas vulnerabilidades han sido fijadas en la versión 6.4.3 Avalanche On-Premise.

Avisos técnicos - Del 5 al 18 de abril

Vulnerabilidades en Mozilla Firefox, Firefox ESR y Thunderbird

Mozilla ha emitido avisos de seguridad donde se tratan múltiples vulnerabilidades que afectan al navegador Firefox 125 y Firefox ESR.

En relación a Firefox 125 destacan 7 vulnerabilidades de severidad alta cuyos identificadores son CVE-2024-3852, CVE-2024-3853, CVE-2024-3854, CVE-2024-3855, CVE-2024-3856, CVE-2024-3857 y CVE-2024-3858. De estas vulnerabilidades, 3 afectan también a Firefox ESR, sus identificadores son CVE-2024-3852, CVE-2024-3854 y CVE-2024-3857.

Avisos técnicos - Del 5 al 18 de abril

Vulnerabilidad de inyección de comandos en Peplink Smart Reader

Matt Wiseman, investigador de Cisco Talos, ha reportado una vulnerabilidad crítica en la interfaz web de Peplink Smart Reader, un sistema para gestionar el acceso a edificios, puestos de trabajo y transporte público, así como para la gestión del tiempo de los empleados.

Avisos técnicos - Del 5 al 18 de abril

Vulnerabilidad de inyección de comandos en productos de Cisco

James Muller ha reportado una vulnerabilidad de severidad alta, cuya explotación podría permitir a un atacante elevar los privilegios a root.

Avisos técnicos - Del 5 al 18 de abril

Vulnerabilidades en Cisco Integrated Management Controller

Cisco ha publicado avisos de seguridad para tratar 2 vulnerabilidades de severidad alta cuyos identificadores son CVE-2024-20295 y CVE-2024-20356, que afectan a Cisco Integrated Management Controller. Su explotación supone una amenaza de alta gravedad para la confidencialidad y la integridad de los sistemas que se vean afectados.

Avisos técnicos - Del 5 al 18 de abril