Del 18 al 28 de septiembre

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

Cross-Site Request Forgery en Free5Gc

INCIBE ha coordinado la publicación de 1 vulnerabilidad que afecta a Free5Gc, un proyecto de código abierto para redes móviles de 5ª generación (5G), la cual ha sido descubierta por Edgar Carrillo Egea.

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

CVE-2023-4659: CVSS v3.1: 9,8 | CVSS: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H | CWE-352.

Avisos técnicos - Del 18 al 28 de septiembre

Vulnerabilidad explotada en enrutador Zyxel

Zyxel ha publicado un aviso de seguridad en el que se trata una vulnerabilidad de severidad alta que afecta al enrutador doméstico Zyxel EMG2926. El identificador de este fallo es el CVE-2017-6884 del que se conoce que está siendo explotado. Dicha explotación implica un alto impacto en la confidencialidad, integridad y disponibilidad de los sistemas afectados.

Vulnerabilidades en Google ChromeOS

Google ha hecho público un aviso de seguridad anunciando una actualización del canal de soporte a largo plazo para ChromeOS. En él se abordan 3 vulnerabilidades de severidad alta cuyos identificadores son CVE-2023-4863, CVE-2023-4572 y CVE-2023-4427, que de ser explotadas supondrían una amenaza de alta gravedad para la confidencialidad, integridad y disponibilidad de los sistemas afectados.

Avisos técnicos - Del 18 al 28 de septiembre

Server-Side Request Forgery en SLiMS

INCIBE ha coordinado la publicación de 1 vulnerabilidad que afecta a SLiMS (Senayan Library Management System), un sistema de gestión de librerías, la cual ha sido descubierta por David Utón Amaya (m3n0sd0n4ld).

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

CVE-2023-3744: CVSS v3.1: 9,9 | CVSS: AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H | CWE-918.

Avisos técnicos - Del 18 al 28 de septiembre

Omisión de autenticación en D-Link D-View 8

Un investigador de Tenable ha descubierto una vulnerabilidad de severidad crítica en el producto D-View de D-Link, cuya explotación podría permitir la omisión de autenticación en dicho producto.

Avisos técnicos - Del 18 al 28 de septiembre

Vulnerabilidad crítica en Drupal

Drupal ha publicado un aviso de seguridad donde se corrige una vulnerabilidad crítica que afecta al módulo JSON:API que se encuentra dentro del core de Drupal. La explotación de este error conduce a condiciones de escalada de privilegios, se puede realizar desde las configuraciones predeterminadas del módulo y produce un impacto de alta gravedad en la confidencialidad de los sistemas afectados.

Avisos técnicos - Del 18 al 28 de septiembre

Múltiples vulnerabilidades en BIND 9

Los investigadores, Eric Sesterhenn, de X41 D-Sec y Robert Story, de USC/ISI DNS, han reportado 2 vulnerabilidades de severidad alta, cuya explotación podría causar una finalización no controlada de las llamadas a la función named.

Avisos técnicos - Del 18 al 28 de septiembre

Múltiples vulnerabilidades en MOVEit Transfer

MOVEit ha publicado una notificación con actualizaciones del Service Pack correspondientes a septiembre 2023, en la que se recogen 3 vulnerabilidades: 2 de severidad alta y 1 media, cuya explotación podría permitir la realización de inyecciones SQL o XSS reflejado.

Avisos técnicos - Del 18 al 28 de septiembre

Vulnerabilidad de escalada de privilegios en el core de Drupal

El investigador Ghostccamm ha reportado una vulnerabilidad de severidad alta que afecta al core de Drupal, cuya explotación podría permitir una escalada de privilegios.

Avisos técnicos - Del 18 al 28 de septiembre

Vulnerabilidades zero-day en Apple

Apple ha publicado diversos avisos de seguridad en los que se abordan vulnerabilidades zero-day, cuyos identificadores son CVE-2023-41991, CVE-2023-41992 y CVE-2023-41993, que afectan al framework de seguridad, al framework del Kernel y al componente WebKit respectivamente, en el navegador Safari y en los sistemas operativos iOS y iPadOS 17, iOS y iPadOS 16, macOS Ventura, macOS Monterey, watchOS 9 y watchOS 10.

Avisos técnicos - Del 18 al 28 de septiembre

Múltiples vulnerabilidades en productos Apple

Bill Marczak, de The Citizen Lab de la Escuela Munk de la Universidad de Toronto, y Maddie Stone, del Google's Threat Analysis Group, han reportado 3 vulnerabilidades que afectan a varios componentes de diversos productos de Apple.

Apple comunica que estas vulnerabilidades afectan a los componentes Kernel, Security y WebKit y están siendo explotadas activamente.

Avisos técnicos - Del 18 al 28 de septiembre

Vulnerabilidades en productos de QNAP

Qnap ha emitido dos avisos de seguridad referentes a vulnerabilidades de severidad alta identificadas como CVE-2023-23363 y CVE-2023-23364. El primer fallo afecta a ciertas versiones heredadas del sistema operativo QTS. El segundo, a ciertas versiones de la consola multimedia. Ambas, de ser explotadas, podrían permitir la ejecución de código, suponiendo una amenaza de alta gravedad para la confidencialidad, integridad y disponibilidad de los sistemas.

Avisos técnicos - Del 18 al 28 de septiembre

Vulnerabilidad de escalada de privilegios local en Driver & Support Assistant de Intel

ZDI, de Trend Micro, ha reportado una vulnerabilidad de severidad alta, cuya explotación podría permitir a un atacante escalar privilegios y ejecutar código arbitrario.

Avisos técnicos - Del 18 al 28 de septiembre

Inyección de comandos OS en EasyPHP Webserver

INCIBE ha coordinado la publicación de 1 vulnerabilidad que afecta a EasyPHP Webserver 14.1, la cual ha sido descubierta por Rafael Pedrero.

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

CVE-2023-3767: CVSS v3.1: 9.8 | CVSS: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H | CWE-78.

Avisos técnicos - Del 18 al 28 de septiembre

Inyección de comandos en el sistema operativo en EasyPHP Webserver

INCIBE ha coordinado la publicación de 1 vulnerabilidad que afecta a EasyPHP Webserver 14.1, la cual ha sido descubierta por Rafael Pedrero.

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

CVE-2023-3767: CVSS v3.1: 9.8 | CVSS: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H | CWE-78.

Avisos técnicos - Del 18 al 28 de septiembre

Vulnerabilidades en Firefox

Mozilla ha emitido un aviso de seguridad donde se tratan 9 vulnerabilidades que afectan al navegador Firefox, Firefox ERS y al cliente de correo electrónico multiplataforma Mozilla Thunderbird. Dentro de estas, destacan 6 de severidad alta cuyos identificadores son CVE-2023-5168, CVE-2023-5169, CVE-2023-5170, CVE-2023-5171, CVE-2023-5172 y CVE-2023-5176, que, de ser explotadas, podrían conducir a condiciones use-after-free, ejecución arbitraria de código, escritura fuera de límites y fuga de memoria.

Avisos técnicos - Del 18 al 28 de septiembre

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 - Del 18 al 28 de septiembre

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 - Del 18 al 28 de septiembre

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 - Del 18 al 28 de septiembre

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 - Del 18 al 28 de septiembre