

Del 11 de noviembre al 5 de
diciembre

AVISOS TÉCNICOS



Vulnerabilidad crítica en productos Atlassian

Atlassian ha publicado un aviso de seguridad en donde se trata la vulnerabilidad crítica de ejecución remota de código, reportada con anterioridad en Apache ActiveMQ, cuyo identificador es CVE-2023-46604, que afecta a los productos Bamboo Data Center y Bamboo Server. El error, de ser explotado, produce un impacto de alta gravedad en la integridad y disponibilidad de los sistemas que se vean afectados.

Avisos técnicos - Del 11 de noviembre al
5 de diciembre

Vulnerabilidad RCE en Red Hat AMQ Broker

Esta vulnerabilidad podría permitir a un atacante remoto ejecutar comandos shell arbitrarios, manipulando tipos de clase serializados en el protocolo OpenWire, haciendo que el broker instancie cualquier clase en el classpath. Se ha asignado el identificador CVE-2023-46604 para esta vulnerabilidad.

Avisos técnicos - Del 11 de noviembre al
5 de diciembre

Múltiples vulnerabilidades en EspoCRM

INCIBE ha coordinado la publicación de 2 vulnerabilidades que afectan a EspoCRM, las cuales han sido descubiertas por Pedro José Navas Pérez de Hispasec. A ambas vulnerabilidades se les han asignado los siguientes códigos, puntuación base CVSS v3.1, vector del CVSS y el tipo de vulnerabilidad CWE de cada vulnerabilidad: CVE-2023-5965 y CVE-2023-5966: CVSS v3.1: 9.1 | CVSS: AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H | CWE-434.

Avisos técnicos - Del 11 de noviembre al
5 de diciembre

Inyección de código en VisualCounter I.Stats

INCIBE ha coordinado la publicación de una vulnerabilidad que afecta a I.Stats de VisualCounter, una herramienta de gestión estadística de datos de afluencia de clientes en zonas comerciales, y que ha sido descubierta por Ignacio García Maestre (Br4v3n). 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-2023-5518: CVSS v3.1: 9.8 | CVSS: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H | CWE-89.

Avisos técnicos - Del 11 de noviembre al
5 de diciembre

Actualización de seguridad de SAP-Noviembre 2023

SAP ha publicado las actualizaciones de seguridad correspondientes al mes de noviembre para una amplia gama de sus productos. En total, se han notificado 3 nuevas notas de seguridad, a las que se añaden 3 actualizaciones de notas publicadas con anterioridad. De todas ellas, 2 se clasifican como de severidad crítica y 4 media, corrigiendo fallos de divulgación de información, falta de autorización, control de acceso inadecuado y falsificación de solicitudes.

Avisos técnicos - Del 11 de noviembre al
5 de diciembre

Actualización de seguridad de SAP de noviembre de 2023

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

Avisos técnicos - Del 11 de noviembre al
5 de diciembre

Múltiples vulnerabilidades en HPE Aruba Access Points

HPE ha publicado 14 vulnerabilidades que afectan a Aruba Access Points, 3 con severidad crítica, 9 altas y 2 medias. La explotación de estas vulnerabilidades podría permitir a un atacante comprometer la integridad del sistema afectado, ejecutar código y comandos arbitrarios, y realizar una denegación de servicio.

Avisos técnicos - Del 11 de noviembre al
5 de diciembre

Omisión de autenticación en VMware Cloud Director Appliance

Dustin Hartle, de Ideal Integrations Inc, ha reportado una vulnerabilidad de severidad crítica, cuya explotación podría permitir a un atacante omitir los mecanismos de autenticación del producto afectado.

Avisos técnicos - Del 11 de noviembre al
5 de diciembre

Actualización de seguridad de Microsoft-Noviembre 2023

Microsoft ha publicado las actualizaciones de seguridad del mes de noviembre de 2023 en las que se corrigen 82 vulnerabilidades, siendo 3 de ellas calificadas como críticas, 56 como importantes, 4 moderadas y 19 sin un valor asignado que afectan al navegador Edge basado en Chromium.

Avisos técnicos - Del 11 de noviembre al
5 de diciembre

Actualizaciones de seguridad de Microsoft de noviembre de 2023

La publicación de actualizaciones de seguridad de Microsoft, correspondiente a la publicación de vulnerabilidades del 14 de noviembre, consta de 63 vulnerabilidades (con CVE asignado), calificadas 2 como críticas, 48 como importantes y como 13 medias.

Avisos técnicos - Del 11 de noviembre al
5 de diciembre

Vulnerabilidad crítica en VMware Cloud Director Appliance

VMware ha publicado un aviso de seguridad para corregir una vulnerabilidad crítica en el producto VMware Cloud Director Appliance, cuyo identificador es CVE-2023-34060. El fallo de omisión de autenticación, de ser explotado, supone una amenaza de alta gravedad para la confidencialidad, integridad y disponibilidad de los sistemas que se vean afectados.

Avisos técnicos - Del 11 de noviembre al
5 de diciembre

Vulnerabilidad de escalada de privilegios en Intel Data Center Manager

Una posible vulnerabilidad de seguridad en el software Intel® Data Center Manager (DCM) podría permitir la elevación de privilegios. Intel está publicando actualizaciones de software para mitigar esta posible vulnerabilidad. Se ha asignado el identificador CVE-2023-31273 para esta vulnerabilidad.

Avisos técnicos - Del 11 de noviembre al
5 de diciembre

Cross-Site Scripting en CKEditor de CKSource

INCIBE ha coordinado la publicación de una vulnerabilidad que afecta a CKEditor, un editor de texto de código abierto que proporciona funciones de procesador de texto en páginas web, y que 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:CVE-2023-4771: CVSS v3.1: 6.1 | CVSS: AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N | CWE-79.

Avisos técnicos - Del 11 de noviembre al
5 de diciembre

Vulnerabilidad en Cisco FTD y FirePOWER Services

Cisco ha publicado un aviso de seguridad para tratar una vulnerabilidad, de severidad alta, en los productos Cisco Firepower Threat Defense Software (FTD) y Cisco FirePOWER Services. El identificador de este error, que puede conducir a una condición de denegación de servicio de ser explotado, es el CVE-2023-20083. El fallo supone una amenaza de alta gravedad para la disponibilidad de los sistemas afectados.

Avisos técnicos - Del 11 de noviembre al
5 de diciembre

Vulnerabilidad XSS en Liferay Portal

Liferay ha publicado una vulnerabilidad crítica de tipo XSS (Cross-Site Scripting) que afecta a su producto Portal.

Avisos técnicos - Del 11 de noviembre al
5 de diciembre

Múltiples vulnerabilidades SQL Buddy

INCIBE ha coordinado la publicación de 6 vulnerabilidades que afectan a SQL Buddy, las cuales han sido descubiertas por Rafael Pedrero. A todas las vulnerabilidades se les ha asignado la siguiente puntuación base CVSS v3.1, vector del CVSS y tipo de vulnerabilidad CWE CVSS v3.1: 6.1 | CVSS: AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N | CWE-79.

Avisos técnicos - Del 11 de noviembre al
5 de diciembre

Múltiples vulnerabilidades en Unitree Robotics A1

INCIBE ha coordinado la publicación de 2 vulnerabilidades que afectan a Unitree Robotics A1 1.16, las cuales han sido descubiertas por Alberto Miguel Diez y Adrián Campazas Vega del Grupo de Robótica de la Universidad de León.

Avisos técnicos - Del 11 de noviembre al
5 de diciembre

Ejecución de código arbitrario en Duet Display

INCIBE ha coordinado la publicación de una vulnerabilidad que afecta a Duet Display 2.5.9.1, una aplicación de escritorio remoto y duplicidad de pantallas, y que ha sido descubierta por Alexander Huamán Jaimes.

Avisos técnicos - Del 11 de noviembre al
5 de diciembre

Vulnerabilidades en Mozilla Firefox y Thunderbird

Mozilla ha emitido avisos de seguridad donde se tratan múltiples vulnerabilidades que afectan al navegador Firefox, Firefox ERS, Firefox para iOS y al cliente de correo electrónico multiplataforma Mozilla Thunderbird. Pueden resultar en condiciones de lectura fuera de límites, Use-After-Free, clickjacking, ejecución remota de código y escalada de privilegios.

Avisos técnicos - Del 11 de noviembre al
5 de diciembre

Limitación incorrecta de una ruta a un directorio restringido en productos de Chameleon Power

INCIBE ha coordinado la publicación de una vulnerabilidad que afecta al framework Malarkey Roof Designer y que ha sido descubierta por Daniel Martínez Adan (adon90), miembro de Holcim EDC.

Avisos técnicos - Del 11 de noviembre al
5 de diciembre

Vulnerabilidades 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 Jira Software Data Center y Server, Confluence Data Server, Crowd Data Center y Server, Bitbucket Data Center y Server y Bamboo Data Center y Server.

Avisos técnicos - Del 11 de noviembre al
5 de diciembre

Múltiples vulnerabilidades en BVRP Software SLmail

INCIBE ha coordinado la publicación de 3 vulnerabilidades que afectan a varios componentes de BVRP Software SLmail, un software de servidor de correo para Microsoft, las cuales han sido descubiertas por Rafael Pedrero.

Avisos técnicos - Del 11 de noviembre al
5 de diciembre

Múltiples vulnerabilidades en productos OwnCloud

Se han publicado 3 vulnerabilidades críticas en productos de OwnCloud, cuya explotación, podría permitir a un atacante provocar una violación de la confidencialidad y la integridad de los datos, así como la de omitir la política de seguridad.

Avisos técnicos - Del 11 de noviembre al
5 de diciembre

Desbordamiento de búfer en Frhed

INCIBE ha coordinado la publicación de una vulnerabilidad que afecta Frhed, un editor de archivos binarios para Windows, que ha sido descubierta por Rafael Pedrero.

Avisos técnicos - Del 11 de noviembre al
5 de diciembre

Vulnerabilidad de elemento de ruta de búsqueda incontrolada en Plesk

INCIBE ha coordinado la publicación de una vulnerabilidad que afecta al instalador de Plesk en su versión 3.27.0.0, una plataforma de gestión de servidores, que ha sido descubierta por Alexander Huaman Jaimes.

Avisos técnicos - Del 11 de noviembre al
5 de diciembre

Múltiples vulnerabilidades en Arcserve UDP

El equipo de Tenable ha notificado al fabricante Arcserve 3 vulnerabilidades críticas que afectan a su producto UDP, cuya explotación podría permitir a un atacante remoto ejecutar código, omitir el proceso de autenticación o acceder a directorios restringidos.

Avisos técnicos - Del 11 de noviembre al
5 de diciembre

Cross-Site Scripting en Alumne LMS

INCIBE ha coordinado la publicación de una vulnerabilidad que afecta la plataforma de e-learning Alumne LMS en su versión 4.0.0.1.08, que ha sido descubierta por Ignacio Lis Malagón.

Avisos técnicos - Del 11 de noviembre al
5 de diciembre

Múltiples vulnerabilidades en NonStop OSS Network Utilities de HPE

HPE ha publicado dos vulnerabilidades de severidad crítica y baja. Estas vulnerabilidades podrían provocar de forma remota la omisión de restricciones de seguridad, vulnerabilidades indirectas y desbordamiento de búfer.

Avisos técnicos - Del 11 de noviembre al
5 de diciembre

Múltiples vulnerabilidades en WinHex

INCIBE ha coordinado la publicación de 2 vulnerabilidades que afectan a distintas versiones de WinHex, un editor hexadecimal universal, las cuales han sido descubiertas por Rafael Pedrero.

Avisos técnicos - Del 11 de noviembre al
5 de diciembre

Vulnerabilidades en Firewalls y Puntos de Acceso de Zyxel

Zyxel ha publicado un aviso de seguridad en el que se tratan un total de 9 vulnerabilidades que afectan a algunas versiones de firewalls y puntos de acceso del fabricante. La más importante, catalogada con una severidad alta, es la que cuenta con el identificador CVE-2023-4398, que, en caso de ser aprovechada, puede ocasionar una condición de denegación de servicio (DoS) a través de ciertos productos, generando un impacto significativo en la disponibilidad de los sistemas afectados.

Avisos técnicos - Del 11 de noviembre al
5 de diciembre

Vulnerabilidad de divulgación de información sensible en productos Netgear

Tenable Network Security ha reportado una vulnerabilidad de severidad crítica que afecta a Prosafe Network Management System de Netgear.

Avisos técnicos - Del 11 de noviembre al
5 de diciembre

[Actualización 30/11/2023]

Vulnerabilidad de divulgación de información sensible en productos Netgear

Tenable Network Security ha reportado una vulnerabilidad de severidad crítica que afecta a Prosafe Network Management System de Netgear.

Avisos técnicos - Del 11 de noviembre al
5 de diciembre

Vulnerabilidad de request smuggling en Apache Tomcat

Norihito Aimoto, investigador de OSSTech Corporation, ha reportado una vulnerabilidad de tipo contrabando de solicitudes (request smuggling) HTTP que afecta a varias versiones de Apache Tomcat.

Avisos técnicos - Del 11 de noviembre al
5 de diciembre

Vulnerabilidades en Google Chrome

Google ha publicado un aviso de seguridad actualizando el canal estable para Windows, Mac y Linux, donde se corrigen 6 vulnerabilidades de severidad alta cuyos identificadores son CVE-2023-6348, CVE-2023-6347, CVE-2023-6346, CVE-2023-6350, CVE-2023-6351 y CVE-2023-6345.

Avisos técnicos - Del 11 de noviembre al
5 de diciembre

Actualizaciones de seguridad de Joomla! 5.0.1 y 4.4.1

El JSST (Joomla! Security Strike Team) ha informado de una vulnerabilidad que afecta al core de Joomla! CMS, cuya explotación podría permitir la divulgación de información.

Avisos técnicos - Del 11 de noviembre al
5 de diciembre

Validación de entrada inadecuada en Newsletter Software SuperMailer

INCIBE ha coordinado la publicación de una vulnerabilidad que afecta al software Newsletter SuperMailer de Mikro Boeer Softwareentwicklungen, en su versión 3.27.0.0, la cual ha sido descubierta por Rafael Pedrero.

Avisos técnicos - Del 11 de noviembre al
5 de diciembre

Múltiples vulnerabilidades en OpenCms de Alkacon Software

INCIBE ha coordinado la publicación de 2 vulnerabilidades que afectan a OpenCms de Alkacon Software, un sistema de gestión de contenidos web de código abierto, las cuales han sido descubiertas por Miguel Segovia Gil.

Avisos técnicos - Del 11 de noviembre al
5 de diciembre

Múltiples vulnerabilidades XSS en productos de BigProf

INCIBE ha coordinado la publicación de 14 vulnerabilidades que afectan a varios productos de BigProf, un sistema de gestión de contenidos web de código abierto, las cuales han sido descubiertas por Rafael Pedrero.

Avisos técnicos - Del 11 de noviembre al
5 de diciembre

Vulnerabilidades en productos NAS de Zyxel

Zyxel ha publicado un aviso de seguridad en el que se tratan un total de 6 vulnerabilidades, de omisión de autenticación e inyección de comandos, que afectan a productos NAS del fabricante. La mayoría de estos fallos, de ser aprovechados, supondrían una amenaza de alta gravedad para la confidencialidad, disponibilidad e integridad de los sistemas.

Avisos técnicos - Del 11 de noviembre al
5 de diciembre

Múltiples vulnerabilidades en Voovi Social Networking Script

INCIBE ha coordinado la publicación de 11 vulnerabilidades que afectan a Voovi, un script de código abierto para redes sociales, las cuales han sido descubiertas por Rafael Pedrero.

Avisos técnicos - Del 11 de noviembre al
5 de diciembre

Vulnerabilidades zero-day en productos Apple

Apple ha publicado varios avisos de seguridad, donde se tratan dos vulnerabilidades zero-day que afectan al componente Webkit en el navegador Safari y los sistemas operativos iOS, iPadOS y macOS Sonoma, que, de ser explotadas, conducen a condiciones de ejecución de código arbitrario y revelación de información confidencial. Desde Apple se afirma tener conocimiento de un informe que indica que estos problemas pueden haber sido explotados activamente en versiones anteriores a iOS 16.7.1.

Avisos técnicos - Del 11 de noviembre al
5 de diciembre

Actualización de seguridad de Android-Diciembre 2023

Google ha publicado las actualizaciones de seguridad de Android del mes de diciembre de 2023, en donde se corrigen 94 vulnerabilidades de las versiones 10, 11, 12, 13 y 14 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.

Avisos técnicos - Del 11 de noviembre al
5 de diciembre