Del 9 al 21 de febrero

AVISOS TÉCNICOS

EUSKO JAURLARITZA
GOBIERNO VASCO

cyber zaintza

Vulnerabilidades críticas en FortiOS y FortiClientEMS

Fortinet ha publicado varios avisos de seguridad para tratar 2 vulnerabilidades de severidad critica, cuyos identificadores son CVE-2024-23113 y CVE-2024-21762, que afectan al producto FortiOS y 1 vulnerabilidad de severidad alta cuyo identificador es CVE-2023-45581, que afecta al producto FortiClientEMS. Estas vulnerabilidades suponen una amenaza de alta gravedad para la confidencialidad, integridad y disponibilidad de los sistemas que se puedan ver afectados.

Avisos técnicos - Del 9 al 21 de febrero

Múltiples vulnerabilidades en FortiOS de Fortinet

Fortinet ha informado de 2 vulnerabilidades críticas que afectan a su sistema operativo FortiOS, una de ellas reportada por Gwendal Guégniaud (CVE-2024-23113). La explotación de las mismas podría permitir a un atacante ejecutar código o comandos no autorizados.

Avisos técnicos - Del 9 al 21 de febrero

[Actualización 12/02/2024] Múltiples vulnerabilidades en FortiOS de Fortinet

Fortinet ha informado de 2 vulnerabilidades críticas que afectan a su sistema operativo FortiOS, una de ellas reportada por Gwendal Guégniaud (CVE-2024-23113). La explotación de las mismas podría permitir a un atacante ejecutar código o comandos no autorizados.

Avisos técnicos - Del 9 al 21 de febrero

Vulnerabilidad de control de acceso inadecuado en Moodle

INCIBE ha coordinado la publicación de una vulnerabilidad de severidad media que afecta a Moodle LMS, un sistema de gestión de aprendizaje, en sus versiones 4.2 y anteriores, la cual ha sido descubierta por David Utón Amaya.

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-2024-1439: 6.5 | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N | CWE-284.

Actualización de seguridad de Microsoft-Febrero 2024

Microsoft ha publicado las actualizaciones de seguridad del mes de febrero de 2024 en las que se corrigen 80 vulnerabilidades, siendo 5 de ellas calificadas como críticas, 66 como importantes, 3 moderadas y 6 sin un valor asignado que afectan al navegador Edge basado en Chromium y a CBL-Mariner, la distribución Linux desarrollada por Microsoft.

Avisos técnicos - Del 9 al 21 de febrero

Vulnerabilidad en archivo OLE2 de ClamAV con impacto en productos Cisco

Cisco ha publicado un aviso de seguridad para tratar una vulnerabilidad, de severidad alta, en el analizador de formato de archivo OLE2 de ClamAV. El identificador de este error, que podría permitir que un atacante remoto no autenticado generar una condición de denegación de servicio, es el CVE-2024-20290. El fallo podría suponer una amenaza de alta gravedad para productos de Cisco con impacto en la confidencialidad, integridad y disponibilidad de los sistemas que se vean afectados.

Avisos técnicos - Del 9 al 21 de febrero

Actualización de seguridad de SAP de febrero de 2024

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

Avisos técnicos - Del 9 al 21 de febrero

Actualizaciones de seguridad de Microsoft de febrero de 2024

La publicación de actualizaciones de seguridad de Microsoft, correspondiente a la publicación de vulnerabilidades del 14 de febrero, consta de 73 vulnerabilidades (con CVE asignado), calificadas 6 como críticas, 52 como importantes, 13 como medias, y 2 como bajas.

Avisos técnicos - Del 9 al 21 de febrero

[Actualización 15/02/2024] Actualizaciones de seguridad de Microsoft de febrero de 2024

La publicación de actualizaciones de seguridad de Microsoft, correspondiente a la publicación de vulnerabilidades del 14 de febrero, consta de 73 vulnerabilidades (con CVE asignado), calificadas 6 como críticas, 52 como importantes, 13 como medias, y 2 como bajas.

Avisos técnicos - Del 9 al 21 de febrero

Actualización de seguridad de SAP-Febrero 2024

SAP ha publicado las actualizaciones de seguridad correspondientes al mes de febrero para una amplia gama de sus productos. En total, se han notificado 13 nuevas notas de seguridad con 3 actualizaciones de notas publicadas con anterioridad. De todas ellas, 2 se clasifican como severidad crítica, 6 como severidad alta, 7 media y 1 como severidad baja, corrigiendo fallos de divulgación de información, Cross-Site Scripting, inyección de código malicioso, inyección de entidad externa XML, validación incorrecta y falta de autorización.

Avisos técnicos - Del 9 al 21 de febrero

Múltiples vulnerabilidades en CMS Made Simple

INCIBE ha coordinado la publicación de 3 vulnerabilidades de severidad crítica que afectan a CMS Made Simple, un sistema de gestión de contenidos (CMS) gratuito y de código abierto (GPL), las cuales han sido descubiertas por Rafael Pedrero.

Avisos técnicos - Del 9 al 21 de febrero

Múltiples vulnerabilidades 0day en productos Autodesk

Se han detectado vulnerabilidades 0day que afectan a varios productos de Autodesk. Las vulnerabilidades afectan a la función de importación de AutoCAD y su explotación requiere la elección interactiva por parte del usuario final.

Avisos técnicos - Del 9 al 21 de febrero

Múltiples vulnerabilidades en SolarWinds Access Rights Manager

Zero Day Initiative, de Trend Micro, en colaboración con un investigador anónimo, han reportado 3 vulnerabilidades de severidad crítica que afectan al producto de control de accesos Access Rights Manager (ARM), del fabricante SolarWinds.

Avisos técnicos - Del 9 al 21 de febrero

Vulnerabilidad de ruta de búsqueda o elemento no citado en Deep Freeze Server Standard de Faronics

IINCIBE ha coordinado la publicación de una vulnerabilidad de severidad media que afecta a Deep Freeze Server Standard, versiones 8.30.020.4627 y anteriores, una herramienta para la protección del disco para entornos informáticos, la cual ha sido descubierta por Rafael Pedrero.

Avisos técnicos - Del 9 al 21 de febrero

Vulnerabilidades en Firewalls y Puntos de Acceso de Zyxel

Zyxel ha publicado un aviso de seguridad donde se exponen 4 vulnerabilidades detectadas de las cuales 2 son de severidad alta, con los identificadores CVE-2023-6764, CVE-2023-6398 y 2 de severidad media que afectan a firewalls y puntos de acceso de este fabricante.

Avisos técnicos - Del 9 al 21 de febrero

Vulnerabilidad de denegación de servicio en Moodle

El investigador, Michael Hawkins, ha reportado una vulnerabilidad de severidad alta que afecta a Moodle.

Avisos técnicos - Del 9 al 21 de febrero

Vulnerabilidades en Mozilla Firefox y Firefox ESR

Mozilla ha emitido avisos de seguridad donde se tratan múltiples vulnerabilidades que afectan al navegador Firefox y Firefox ERS. Dentro de estas, destacan 4 de severidad alta cuyos identificadores son CVE-2024-1546, CVE-2024-1547, CVE-2024-1553, CVE-2024-1557, que, de ser explotadas, pueden resultar en condiciones de lectura de memoria fuera de límites y corrupción de memoria, entre otros.

Avisos técnicos - Del 9 al 21 de febrero

Vulnerabilidades de alto impacto en VMware Enhanced Authentication Plug-in

VMware ha publicado un aviso de seguridad relativo a dos vulnerabilidades, una de severidad crítica, CVE-2024-22245 y otra alta, CVE-2024-22250, que afectan al producto VMware Enhanced Authentication Plug-in (EAP). Cabe destacar que este plugin se encuentra obsoleto desde 2021 debido al lanzamiento de vCenter Server 7.0u2.

Múltiples vulnerabilidades en productos de Liferay

Liferay ha publicado varias vulnerabilidades de diferentes severidades, de las cuales 11 son críticas y podrían permitir a un atacante inyectar secuencias de comandos de forma remota (XSS).

Avisos técnicos - Del 9 al 21 de febrero

[Actualización 22/02/2024] Múltiples vulnerabilidades en productos de Liferay

Liferay ha publicado varias vulnerabilidades de diferentes severidades, de las cuales 11 son críticas y podrían permitir a un atacante inyectar secuencias de comandos de forma remota (XSS).

Avisos técnicos - Del 9 al 21 de febrero

Múltiples vulnerabilidades en VMware Enhanced Authentication Plug-in

Ceri Coburn, de Pen Test Partners, ha reportado 2 vulnerabilidades, de severidad crítica y alta respectivamente, en el producto deprecated Enhanced Authentication Plug-in (EAP) de VMware.

Avisos técnicos - Del 9 al 21 de febrero

Vulnerabilidades en productos de Atlassian

Atlassian ha publicado su actualización de seguridad mensual donde se tratan 9 vulnerabilidades de severidad alta que afectan a los productos Confluence Data Center y Server, Jira Software Data Center y Server, Assets Discovery, Jira Service Management Data Center y Server.

Avisos técnicos - Del 9 al 21 de febrero

Múltiples vulnerabilidades en ConnectWise ScreenConnect

ConnectWise Control, conocido anteriormente como Screenconnect, contiene 2 vulnerabilidades, una de severidad crítica y otra alta, cuya explotación podría permitir la ejecución de código remoto o directamente impactar en la confidencialidad de la información o en sistemas críticos.

Avisos técnicos - Del 9 al 21 de febrero

Vulnerabilidades en Google Chrome

Google ha publicado un aviso de seguridad actualizando el canal de asistencia actualizando a la versión 122.0.6261.57/58 para Windows y 122.0.6261.57 para Linux y Mac donde se corrigen 8 vulnerabilidades de las cuales 2 son consideradas como severidad alta cuyos identificadores son CVE-2024-1669 y CVE-2024-1670, 5 consideradas con severidad media, cuyos identificadores son CVE-2024-1671, CVE-2024-1672, CVE-2024-1673, CVE-2024-1674, CVE-2024-1675 y 1 con severidad baja cuyo identificador es CVE-2024-1676.

Avisos técnicos - Del 9 al 21 de febrero