

Del 13 al 21 de marzo

AVISOS TÉCNICOS



Actualización de seguridad de Microsoft-Marzo 2024

Microsoft ha publicado las actualizaciones de seguridad del mes de marzo de 2024 en las que se corrigen 63 vulnerabilidades, siendo 2 de ellas calificadas como críticas, 57 como importantes y 4 sin un valor asignado que afectan al navegador Edge basado en Chromium y a Microsoft Edge para Android.

Avisos técnicos - Del 13 al 21 de marzo

Actualización de seguridad de SAP-Marzo 2024

SAP ha publicado las actualizaciones de seguridad correspondientes al mes de marzo 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 crítica, 3 como severidad alta, y 6 como severidad media, corrigiendo fallos de inyección de código malicioso, autenticación incorrecta, denegación de servicio (DDoS), recorrido de ruta, Cross-Site Scripting (XSS), divulgación de información y falta verificación de autorización.

Avisos técnicos - Del 13 al 21 de marzo

Actualización de seguridad de SAP de marzo de 2024

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

Avisos técnicos - Del 13 al 21 de marzo

Múltiples vulnerabilidades en router Movistar 4G

INCIBE ha coordinado la publicación de 3 vulnerabilidades: dos de severidad alta y una de severidad media, que afectan al router Movistar 4G, dispositivo hardware que permite la conexión a Internet, versión ES_WLD71-T1_v2.0.201820, las cuales han sido descubiertas por Gabriel Gonzalez García.

Avisos técnicos - Del 13 al 21 de marzo

Actualizaciones de seguridad de Microsoft de marzo de 2024

La publicación de actualizaciones de seguridad de Microsoft, correspondiente a la publicación de vulnerabilidades del 12 de febrero, consta de 61 vulnerabilidades (con CVE asignado), calificadas 2 como críticas que afectan a Windows Hyper-V, y el resto importantes.

Avisos técnicos - Del 13 al 21 de marzo

Vulnerabilidades críticas en FortiOS y FortiClientEMS

Fortinet ha publicado varios avisos de seguridad para tratar 3 vulnerabilidades de severidad crítica, cuyos identificadores son CVE-2023-42789, CVE-2023-42790 y CVE-2023-48788, las cuales afectan al producto FortiOS, y 3 vulnerabilidades de severidad alta, cuyos identificadores son CVE-2023-47534, CVE-2024-23112 y CVE-2023-36554, las cuales afectan al producto FortiClientEMS.

Avisos técnicos - Del 13 al 21 de marzo

Vulnerabilidades en Cisco IOS-XR

Cisco ha publicado avisos de seguridad para tratar 3 vulnerabilidades, de severidad alta, que afectan al producto Cisco IOS-XR, el sistema operativo de equipos de red del fabricante, con los identificadores CVE-2024-20318, CVE-2024-20320 y CVE-2024-20327. Estas vulnerabilidades suponen una amenaza de alta gravedad con impacto en la confidencialidad, la disponibilidad y la integridad de los sistemas que se vean afectados.

Avisos técnicos - Del 13 al 21 de marzo

Vulnerabilidad de expiración de sesión insuficiente en router Sagemcom

INCIBE ha coordinado la publicación de una vulnerabilidad de severidad alta que afecta al router FAST3686 V2 Vodafone (fabricado por Sagemcom), dispositivo hardware que permite el acceso a Internet, la cual ha sido descubierta por David Utón.

Vulnerabilidad de uso de clave criptográfica en texto plano en FriendlyWrt de FriendlyElec

INCIBE ha coordinado la publicación de una vulnerabilidad de severidad media que afecta a FriendlyWrt, versión 2022-11-16.51b3d35, un sistema personalizado hecho por FriendlyElec basado en una distribución OpenWrt, la cual ha sido descubierta por HADESS.

Múltiples vulnerabilidades en AMSS++ de Amssplus

INCIBE ha coordinado la publicación de 16 vulnerabilidades que afectan a AMSS++, herramienta para el sistema de apoyo a la gestión de oficinas del área de servicios educativos, de Amssplus: 1 de severidad crítica y 15 de severidad alta, las cuales han sido descubiertas por Rafael Pedrero.

Avisos técnicos - Del 13 al 21 de marzo

Múltiples vulnerabilidades en Alma Blog de Devklan

INCIBE ha coordinado la publicación de 3 vulnerabilidades de severidad media que afectan a Alma Blog de Devklan, plataforma de blogs destinada principalmente a la creación de sitios web, blogs o comunidades de noticias o temáticos, versiones 2.1.10 y anteriores, las cuales han sido descubiertas por David Utón Amaya.

Avisos técnicos - Del 13 al 21 de marzo

Múltiples vulnerabilidades en Meta4 HR de Cegid

INCIBE ha coordinado la publicación de 5 vulnerabilidades, una de severidad crítica, dos altas y dos medias que afectan a Meta4 HR del fabricante Cegid, las cuales han sido descubiertas por:

Pedro Jose Navas Pérez, de Hispasec, y Jesús Antón (CVE-2024-2632).

Pedro Jose Navas Pérez, de Hispasec, (CVE-2024-2633 y CVE-2024-2634).

Jesús Antón (CVE-2024-2635 y CVE-2024-2636).

Avisos técnicos - Del 13 al 21 de marzo

Recorrido de ruta en EVO de Franklin Fueling System

Momen Eldawakhly, de Samurai Digital Security Ltd, ha informado de una vulnerabilidad de severidad alta que podría permitir a un atacante leer archivos arbitrarios en el sistema.

Avisos técnicos - Del 13 al 21 de marzo

Vulnerabilidades en Mozilla Firefox, Firefox ESR y Thunderbird

Mozilla ha emitido avisos de seguridad donde se tratan múltiples vulnerabilidades que afectan al navegador Firefox, Firefox ERS y al cliente de correo electrónico multiplataforma Mozilla Thunderbird.

Avisos técnicos - Del 13 al 21 de marzo

Múltiples vulnerabilidades en el sistema CIGESv2

INCIBE ha coordinado la publicación de 7 vulnerabilidades, 3 de severidad crítica, 1 de severidad alta y 3 de severidad media, que afectan al sistema de gestión de colas y citas previas CIGESv2, las cuales han sido descubiertas por:

Óscar Atienza (CVE-2024-2722, CVE-2024-2723 y CVE-2024-2724).

Rubén López Herrera (CVE-2024-2725, CVE-2024-2726, CVE-2024-2727 y CVE-2024-2728).

Avisos técnicos - Del 13 al 21 de marzo

Vulnerabilidades en productos de Atlassian

Atlassian ha publicado su actualización de seguridad mensual donde se tratan múltiples vulnerabilidades, una de severidad crítica y varias alta, las cuales afectan a los productos Bamboo Data Center and Server, Bitbucket Data Center and Server y Confluence Data Center and Server.

Avisos técnicos - Del 13 al 21 de marzo

Vulnerabilidad de inyección de SQL en SCAN_VISIO eDocument Suite Web Viewer de Abast

INCIBE ha coordinado la publicación de una vulnerabilidad que afecta a SCAN_VISIO Web Viewer, un módulo de la solución SCAN_VISIO eDocument Suite, la cual ha sido descubierta por Alberto Gasulla y Ismael Pacheco Torrecilla.

Múltiples vulnerabilidades en productos Ivanti

Ivanti ha notificado 2 vulnerabilidades de severidad crítica que afectan a sus productos Neurons para ITSM y Standalone Sentry, respectivamente. La explotación de ambas vulnerabilidades podría permitir a un atacante remoto modificar un archivo o ejecutar código.

Avisos técnicos - Del 13 al 21 de marzo

Vulnerabilidades críticas en productos de Ivanti

Ivanti ha publicado avisos de seguridad para tratar 2 vulnerabilidades de severidad crítica, CVE-2023-46808 de escritura remota de archivos autenticada y CVE-2023-41724 de ejecución remota de código que afectan a los productos Ivanti Neurons para ITSM e Ivanti Standalone Sentry, respectivamente. Los fallos suponen una amenaza de gravedad crítica con impacto en la confidencialidad, integridad y disponibilidad de los sistemas que se vean afectados.

Avisos técnicos - Del 13 al 21 de marzo

Múltiples vulnerabilidades en Sentrifugo

INCIBE ha coordinado la publicación de 10 vulnerabilidades, 7 de severidad crítica y 3 de severidad alta, que afectan a Sentrifugo versión 3.2, un sistema de gestión de recursos humanos, las cuales han sido descubiertas por Rafael Pedrero.

Avisos técnicos - Del 13 al 21 de marzo