Hasta el 2 de mayo

AVISOS TÉCNICOS

EUSKO JAURLARITZA
GOBIERNO VASCO

cyber zaintza

Vulnerabilidad en Citrix uberAgent

Citrix ha publicado un aviso de seguridad para tratar 1 vulnerabilidad de severidad alta cuyo identificador es CVE-2024-3902 que afecta al producto Citrix uberAgent. Su explotación puede dar lugar a una condición de escalada de privilegios con impacto en la confidencialidad e integridad de los sistemas que se vean afectados.

Avisos técnicos - Hasta el 2 de mayo

Actualización de seguridad de Oracle-Abril 2024

Oracle ha publicado su boletín trimestral de actualizaciones de seguridad, que aborda 441 correcciones en una amplia variedad de productos. La mayoría de estos fallos permiten a un atacante remoto comprometer la integridad, confidencialidad y disponibilidad de los sistemas afectados, lo que podría dar lugar a la pérdida de datos y la interrupción de los servicios.

Avisos técnicos - Hasta el 2 de mayo

Inyección de comandos en productos Cisco

Cisco ha publicado una vulnerabilidad de severidad alta que podría permitir que un atacante remoto autenticado con privilegios de nivel de administrador, realice ataques de inyección de comandos en un sistema afectado y eleve sus privilegios a root.

Avisos técnicos - Hasta el 2 de mayo

Cross-Site Scripting en la aplicación Holded

INCIBE ha coordinado la publicación de una vulnerabilidad de severidad media que afecta al aplicativo Holded, un software de gestión para PYMES y emprendedores, la cual ha sido descubierta por Raúl Vega Arjona, de Hispasec Sistemas.

Avisos técnicos - Hasta el 2 de mayo

Múltiples vulnerabilidades en Hyperion Web Server

INCIBE ha coordinado la publicación de 2 vulnerabilidades de severidad media que afectan a Hyperion, un software de luz ambiental de código abierto, versión 2.0.15 las cuales han sido descubiertas por Raúl Fuentes Ferrer.

Avisos técnicos - Hasta el 2 de mayo

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 corrige 1 vulnerabilidad de severidad crítica, cuyo identificador es CVE-2024-4058 y 2 de severidad alta cuyos identificadores son CVE-2024-4059 y CVE-2024-4060.

Avisos técnicos - Hasta el 2 de mayo

Vulnerabilidades en Cisco Adaptive Security Appliance y Firepower Threat Defense

Cisco ha publicado avisos de seguridad para tratar 2 vulnerabilidades de severidad alta cuyos identificadores son CVE-2024-20353 y CVE-2024-20359, que afectan a los productos Cisco Adaptive Security Appliance y Firepower Threat Defense.

Avisos técnicos - Hasta el 2 de mayo

Múltiples vulnerabilidades en switches SAN de HPE

HPE ha publicado 6 vulnerabilidades, 1 de severidad crítica, 1 de severidad alta, y 4 de severidad media que podrían ser explotadas de forma remota o local.

Avisos técnicos - Hasta el 2 de mayo

Vulnerabilidad RCE en Wazuh Manager

Konstantin Bücheler (d0ntrash) ha reportado una vulnerabilidad de severidad crítica en Wazuh Manager. La explotación de esta vulnerabilidad podría permitir a un atacante remoto ejecutar código.

Avisos técnicos - Hasta el 2 de mayo

Vulnerabilidad en la plataforma SWAL de GT3 Soluciones

INCIBE ha coordinado la publicación de una vulnerabilidad de severidad media que afecta a SWAL de GT3 Soluciones versión 2.0 (r2301), un software para la gestión de la administración local, la cual ha sido descubierta por David Padilla.

Avisos técnicos - Hasta el 2 de mayo

Múltiples vulnerabilidades en HubBank

INCIBE ha coordinado la publicación de 5 vulnerabilidades, 1 de severidad crítica, tres de severidad alta y 1 de severidad media, que afectan a HubBank de Ofofonobs versión 1.0.2, un script de banca online con notificaciones por SMS y correo electrónico, las cuales han sido descubiertas por David Utón Amaya.

Avisos técnicos - Hasta el 2 de mayo

Múltiples vulnerabilidades en Adive Framework

INCIBE ha coordinado la publicación de 2 vulnerabilidades de severidad alta que afectan a Adive Framework, un generador web y de paneles de administración, las cuales han sido descubiertas por Rafael Pedrero.

Avisos técnicos - Hasta el 2 de mayo

Ejecución de código arbitrario en lenguaje de programación R

Kasimir Schulz y Kieran Evans, investigadores de HiddenLayer, han reportado una vulnerabilidad de severidad alta en el lenguaje R que podría permitir ejecutar código arbitrario directamente tras la deserialización de datos no fiables, permitiendo a un atacante tomar el control del sistema afectado.

La investigación de HiddenPlayer ha detectado repositorios con ficheros fuente que potencialmente podrían contener código vulnerable incluidos en proyectos de R Studio, Facebook, Google, Microsoft, AWS y otros proveedores de software.

Avisos técnicos - Hasta el 2 de mayo

Múltiples vulnerabilidades en ArubaOS de HPE Aruba

HPE ha publicado 10 vulnerabilidades: 4 de severidad crítica y 6 medias, que podrían dar lugar a una ejecución de código arbitrario y denegación de servicio (DoS).

Avisos técnicos - Hasta el 2 de mayo