

Hasta el 4 de abril

AVISOS TÉCNICOS



EUSKO JAURLARITZA
GOBIERNO VASCO

 cyber
zaintza

Múltiples vulnerabilidades en productos de DELL

Dell ha publicado 2 vulnerabilidades de severidades crítica y media que podrían provocar la pérdida de confidencialidad, integridad y disponibilidad.

Avisos técnicos - Hasta el 4 de abril

Denegación de servicio en Punto de Acceso de Cisco

Cisco ha publicado una vulnerabilidad de severidad alta que podría permitir que un atacante remoto, no autenticado, cause una condición de denegación de servicio (DoS) en un dispositivo afectado.

Avisos técnicos - Hasta el 4 de abril

Inyección de código malicioso en la librería XZ Utils

Andres Freund, ingeniero de software de Microsoft, ha descubierto una vulnerabilidad crítica en XZ Utils, una librería de compresión de datos ampliamente utilizada en varias distribuciones de Linux. En las versiones 5.6.0 y 5.6.1 se introdujo código malicioso. XZ Utils que incluye la librería liblzma utilizado por varios software, incluyendo sshd que es una de las técnicas conocidas para abusar del backdoor instalado.

Avisos técnicos - Hasta el 4 de abril

Vulnerabilidades de severidad alta en VMware

VMware ha publicado un aviso de seguridad relativo a 2 vulnerabilidades de severidad alta, con los identificadores CVE-2024-22246, CVE-2024-22248, y 1 vulnerabilidad de severidad media, con el identificador CVE-2024-22247, las cuales afectan a los productos VMware SD-WAN Edge y VMware SD-WAN Orchestrator.

Avisos técnicos - Hasta el 4 de abril

Actualización de seguridad de Apple-Marzo 2024

A lo largo del mes de marzo, Apple ha publicado 18 actualizaciones de seguridad en las que se corrigen 83 vulnerabilidades que afectan a los sistemas operativos iOS, iPadOS, macOS Sonoma, macOS Ventura, macOS Monterey, tvOS, watchOS, visionOS, a la aplicación GarageBand, a XCode y al navegador Safari.

Avisos técnicos - Hasta el 4 de abril

Vulnerabilidades en Ivanti Connect Secure e Ivanti Policy Secure

Ivanti ha publicado un aviso de seguridad para tratar vulnerabilidades de severidad alta en los productos Ivanti Connect Secure (ICS) e Ivanti Policy Secure, con los identificadores CVE-2024-21894, CVE-2024-22052, CVE-2024-22053. También se corrige un fallo de severidad media, CVE-2024-22023. Todos estos errores tienen impacto en la disponibilidad de los sistemas que se vean afectados.

Avisos técnicos - Hasta el 4 de abril

Vulnerabilidad en Cisco Nexus Dashboard Controller

Cisco ha publicado aviso de seguridad para tratar 1 vulnerabilidad de severidad alta que afecta a Cisco Nexus Dashboard Fabric Controller. El identificador de esta vulnerabilidad es CVE-2024-20348. Su explotación supone una amenaza de alta gravedad para la confidencialidad de los sistemas que se vean afectados.

Avisos técnicos - Hasta el 4 de abril

Actualización de seguridad de Android-Abril 2024

Google ha publicado las actualizaciones de seguridad de Android y dispositivos Píxel del mes de abril de 2024, donde se corrigen 53 vulnerabilidades, que abarcan soluciones para fallos de elevación de privilegios, divulgación de información y denegación de servicio.

Avisos técnicos - Hasta el 4 de abril

Vulnerabilidad de exposición de información en Request Tracker (RT)

INCIBE ha coordinado la publicación de una vulnerabilidad de severidad media que afecta a RT versión 4.4.1, herramienta desarrollada por Best Practical Solutions para la gestión de ciberincidentes, la cual ha sido descubierta por Javier Garcia Antón.

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-2024-3262:	5.5	
CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N		
CWE-200		

Avisos técnicos - Hasta el 4 de abril