

Del 3 al 12 de abril

# AVISOS TÉCNICOS



# Actualizaciones de seguridad de Apple-Marzo 2023

---

A lo largo del mes de marzo, Apple ha publicado 12 actualizaciones de seguridad en las que se corrigen 70 fallos que afectan al entorno de desarrollo Xcode, a la línea de monitores Studio Display, al navegador Safari, a los sistemas operativos iOS, macOS Ventura, watchOS, iPadOS y tvOS, y por último, a la aplicación de software de música y producción musical GarageBand.

Avisos técnicos - Del 3 al 12 de abril

# Fuga de información en impresoras HP

---

HP ha informado de una vulnerabilidad crítica que afecta a varios modelos de HP Enterprise LaserJet y HP LaserJet Managed Printers, cuya explotación podría permitir la divulgación de información.

Avisos técnicos - Del 3 al 12 de abril

# Boletín de seguridad de Android de abril de 2023

---

El boletín de Android, relativo a abril de 2023, soluciona múltiples vulnerabilidades de severidad crítica, alta y moderada, que afectan al sistema operativo Android, así como a múltiples componentes, y que podrían permitir a un atacante realizar una escalada de privilegios, divulgar información y provocar una denegación de servicio (DoS) o una ejecución de código remota (RCE).

Avisos técnicos - Del 3 al 12 de abril

# Vulnerabilidades en Sophos Web Appliance

---

Sophos ha publicado un aviso de seguridad donde se tratan 3 vulnerabilidades CVE-2023-1671, CVE-2022-4934, CVE-2020-36692, de severidades crítica, alta y media respectivamente.

Avisos técnicos - Del 3 al 12 de abril

# Actualización de seguridad de Android-Abril 2023

---

Google ha publicado las actualizaciones de seguridad para Android del mes de abril de 2023 en donde se corrigen 66 vulnerabilidades de las versiones 10, 11, 12 y 13 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. De las 66 vulnerabilidades tratadas, 6 tiene severidad crítica, 59 alta y 1 moderada.

Avisos técnicos - Del 3 al 12 de abril

# Vulnerabilidades en Cisco Expressway y Cisco VCS

---

Cisco ha publicado un aviso de seguridad donde se tratan 2 vulnerabilidades, CVE-2022-20812 de severidad crítica y CVE-2022-20813 de severidad alta, que afectan a la API y la interfaz de administración basada en la web de Cisco Expressway Series y Cisco TelePresence Video Communication Server (VCS) respectivamente. Estas vulnerabilidades podrían permitir que un atacante remoto sobrescriba archivos arbitrarios o realice ataques de envenenamiento de bytes nulos en un dispositivo.

Avisos técnicos - Del 3 al 12 de abril

# Ransomware Rorschach impacta en producto Cortex XDR de Palo Alto Networks

---

El equipo de Product Security Assurance, de Palo Alto Networks, tiene conocimiento de un artículo que detalla una variante de ransomware denominada Rorschach, que podría afectar a varias versiones del agente Cortex XDR ejecutadas en entornos Windows.

Avisos técnicos - Del 3 al 12 de abril



# Múltiples vulnerabilidades en productos HP LaserJet Pro

---

Los equipos de DEVCORE Research Team y Neodyme, en colaboración con Trend Micro ZDI, han reportado 3 vulnerabilidades de severidad alta en impresoras LaserJet Pro de HP.

Avisos técnicos - Del 3 al 12 de abril

# Vulnerabilidades en productos de Apple

---

Clément Lecigne del Grupo de Análisis de Amenazas de Google y Donncha Ó Cearbhaill del Laboratorio de Seguridad de Amnistía Internacional han notificado 2 vulnerabilidades, cuya explotación podría permitir ejecutar código arbitrario.

Avisos técnicos - Del 3 al 12 de abril

# Vulnerabilidades zero-day en productos de Apple

---

Apple ha publicado diversos avisos de seguridad, en los que se abordan dos vulnerabilidades de tipo zero-day que se deben a dos errores existentes en los componentes WebKit e IOSurfaceAccelerator respectivamente, afectando a los sistemas operativos iOS, iPadOS, macOS Ventura, macOS Monterey y macOS Big Sur. Las vulnerabilidades, cuyos identificadores son CVE-2023-28205 y CVE-2023-28206, de momento no tienen asignada una puntuación de acuerdo a la escala CVSSv3, pero han sido calificadas por el fabricante como de tipo zero-day, por lo tanto se les asigna una severidad crítica.

Avisos técnicos - Del 3 al 12 de abril

# Actualización de seguridad de Microsoft-Abril 2023

---

Microsoft ha publicado las actualizaciones de seguridad del mes de abril de 2023 en las que se corrigen 114 vulnerabilidades, siendo 7 de ellas calificadas como críticas, 90 como importantes, 1 moderada, 2 bajas y 14 sin un valor asignado que corrigen problemas en el navegador Edge basado en Chromium.

Dentro de ellas existe 1 vulnerabilidad zero-day que está siendo explotada, cuyo identificador es CVE-2023-28252.

Avisos técnicos - Del 3 al 12 de abril

# Actualizaciones de seguridad de Microsoft de abril de 2023

---

La publicación de actualizaciones de seguridad de Microsoft, correspondiente al mes de abril y que incluye toda la información comprendida entre los días 15/03/2023 y 11/04/2023, consta de 124 vulnerabilidades (con CVE asignado), calificadas como: 7 de severidad crítica, 90 importantes, 2 moderadas, 4 bajas y 21 sin severidad asignada.

Avisos técnicos - Del 3 al 12 de abril

# Actualización de seguridad de SAP de abril de 2023

---

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

Avisos técnicos - Del 3 al 12 de abril

# Vulnerabilidades en productos de Fortinet

---

Fortinet ha publicado varias actualizaciones de seguridad donde las más relevantes tratan fallos de severidad crítica y alta. En el aviso FG-IR-22-355 se trata un fallo crítico, con el identificador CVE-2022-41331, que afecta al producto FortiPresence. En los restantes FG-IR-22-050, FG-IR-22-335, FG-IR-22-336, FG-IR-22-429, FG-IR-22-320, FG-IR-22-363, FG-IR-23-051, FG-IR-22-056 y FG-IR-22-428 se abordan varios problemas de severidad alta, cuyos identificadores son CVE-2022-0847, CVE-2022-40679, CVE-2022-40682, CVE-2022-43946, CVE-2022-42470, CVE-2022-41330, CVE-2023-27995, CVE-2022-27487, CVE-2022-43955.

Avisos técnicos - Del 3 al 12 de abril

# Vulnerabilidades en productos de Adobe

---

Adobe ha publicado un total de seis avisos de seguridad en los que se abordan un total de 56 vulnerabilidades relacionadas con Adobe Digital Editions, Adobe InCopy, Adobe Acrobat and Reader, Adobe Substance 3D Stager, Adobe Substance 3D Designer y Adobe Dimension. Entre todas ellas, se destacan un total de 49 vulnerabilidades que han sido calificadas con una severidad crítica por parte de la compañía.

Avisos técnicos - Del 3 al 12 de abril