

Del 12 al 22 de junio

AVISOS TÉCNICOS



Vulnerabilidad RCE en dispositivos Fortigate SSL-VPN de Fortinet

Se ha identificado una vulnerabilidad crítica de ejecución remota de código (RCE) previa a la autenticación en productos Fortigate de Fortinet.

Avisos técnicos - Del 12 al 22 de junio

[Actualización 13/06/2023] Vulnerabilidad RCE en dispositivos Fortigate SSL-VPN de Fortinet

[Actualización 13/06/2023] Los investigadores Charles Fol y Dany Bach, de LEXFO, han identificado una vulnerabilidad crítica de ejecución remota de código (RCE) previa a la autenticación en varios productos de Fortinet.

Avisos técnicos - Del 12 al 22 de junio

Desbordamiento de búfer y ejecución remota de código en Enterprise LaserJet MFP de HP

HP ha notificado una vulnerabilidad de severidad crítica que podría provocar un desbordamiento de búfer o una ejecución remota de código.

Avisos técnicos - Del 12 al 22 de junio

Actualización de seguridad de SAP-Junio 2023

SAP ha publicado las actualizaciones de seguridad correspondientes al mes de junio para una amplia gama de sus productos. En total, se han notificado 8 nuevas notas de seguridad a las que se añaden 5 actualizaciones de notas publicadas con anterioridad. De todas ellas, 4 se clasifican como de severidad alta, 8 como medias y 1 como baja, corrigiendo fallos de denegación de servicio, Cross-Site Scripting (XSS), divulgación de información e inyección SQL entre otros.

Avisos técnicos - Del 12 al 22 de junio

Vulnerabilidades en productos Fortinet

Fortiguard, organización de investigación de amenazas dirigidas a productos de Fortinet, ha publicado un total de 21 avisos de seguridad que afectan a diversos productos del fabricante.

Avisos técnicos - Del 12 al 22 de junio

Actualización de seguridad de Microsoft-Junio 2023

Microsoft ha publicado las actualizaciones de seguridad del mes de junio de 2023 en las que se corrigen 94 vulnerabilidades, siendo 6 de ellas calificadas como críticas, 69 como importantes, 3 moderadas, 2 bajas y 14 sin un valor asignado. Estas últimas corrigen problemas en el navegador Edge basado en Chromium.

Avisos técnicos - Del 12 al 22 de junio

Vulnerabilidad crítica en Citrix ShareFile Storage

Citrix ha publicado un aviso de seguridad donde se aborda una vulnerabilidad crítica, cuyo identificador es CVE-2023-24489, que afecta al servicio en la nube ShareFile storage. El error consiste en un fallo de control de acceso inadecuado y su explotación podría suponer una amenaza de alta gravedad para la confidencialidad, integridad y disponibilidad de los sistemas afectados.

Avisos técnicos - Del 12 al 22 de junio

Control de acceso inadecuado en ShareFile de Citrix

Dylan Pindur, investigador de Assetnote, ha reportado una vulnerabilidad crítica que afecta al controlador de zonas de almacenamiento ShareFile gestionado por el cliente.

Avisos técnicos - Del 12 al 22 de junio

Vulnerabilidades en Google Chrome

Google ha hecho público un aviso de seguridad anunciando una actualización del escritorio en canal estable para Google Chrome en sistemas Mac, Linux y Windows. En él se abordan 4 vulnerabilidades, 1 crítica con identificador CVE-2023-3214 y 3 de severidad alta, cuyos identificadores son CVE-2023-3215, CVE-2023-3216, CVE-2023-3217.

Avisos técnicos - Del 12 al 22 de junio

Actualización de seguridad de SAP de junio de 2023

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

Avisos técnicos - Del 12 al 22 de junio

Actualizaciones de seguridad de Microsoft de junio de 2023

La publicación de actualizaciones de seguridad de Microsoft, correspondiente a la publicación de vulnerabilidades del 13 de junio, consta de 78 vulnerabilidades (con CVE asignado), calificadas como: 6 de severidad crítica y 72 importantes.

Avisos técnicos - Del 12 al 22 de junio

Escalada de privilegios en productos Pulse Secure

La vulnerabilidad de severidad alta podría permitir a un atacante local aumentar los privilegios en las instalaciones afectadas de Pulse Secure Client.

Avisos técnicos - Del 12 al 22 de junio

Vulnerabilidad de escalada de privilegios en MOVEit Transfer de Progress

Progress ha notificado una vulnerabilidad crítica en su producto MOVEit Transfer.

Avisos técnicos - Del 12 al 22 de junio

Vulnerabilidad crítica en productos NAS de Zyxel

Zyxel ha publicado un aviso de seguridad donde se trata una vulnerabilidad crítica, cuyo identificador es CVE-2023-27992, que afecta a los dispositivos de almacenamiento en la nube (NAS) Zyxel NAS326, NAS540 y NAS542.

Avisos técnicos - Del 12 al 22 de junio

Ejecución de código en Endpoint Manager de Ivanti

Ivanti ha publicado en su aviso de seguridad una vulnerabilidad de severidad alta, la cual podría permitir a un atacante realizar un aumento de privilegios y una ejecución remota de código.

Avisos técnicos - Del 12 al 22 de junio

Vulnerabilidad TOCTOU en el firmware AMI UEFI de PC HP

Los investigadores de Intel iStare Jonathan Lusky y Benny Zeltser han reportado una vulnerabilidad de severidad alta que podría permitir la ejecución de código arbitrario.

Avisos técnicos - Del 12 al 22 de junio

Múltiples vulnerabilidades 0day en productos de Apple

Georgy Kucherin, Leonid Bezvershenko y Boris Larin, de Kaspersky, han informado a Apple 3 sobre vulnerabilidades 0day que podrían permitir a un atacante ejecutar código arbitrario.

Avisos técnicos - Del 12 al 22 de junio

Vulnerabilidades zero-day en Apple

Apple ha publicado diversos avisos de seguridad, en los que se abordan vulnerabilidades zero-day, cuyos identificadores son CVE-2023-32439, CVE-2023-32435 y CVE-2023-32434 que afectan al componente WebKit en el navegador Safari además del Kernel de los sistemas operativos iOS, iPadOS, macOS Ventura, macOS Monterey, macOS Big Sur, watchOS.

Avisos técnicos - Del 12 al 22 de junio

Vulnerabilidades en VMware

VMware ha publicado un aviso de seguridad que aborda 5 vulnerabilidades, CVE-2023-20892, CVE-2023-20893, CVE-2023-20894 y CVE-2023-20895 de severidad alta y CVE-2023-20896 de severidad media. Los fallos de mayor gravedad se corresponden con errores de desbordamiento del heap, Use-After-Free, escritura fuera de límites y corrupción de memoria, suponiendo la explotación de todas ellas una amenaza significativa para la confidencialidad, disponibilidad e integridad de los sistemas afectados.

Avisos técnicos - Del 12 al 22 de junio