

Hasta el 3 de agosto

AVISOS TÉCNICOS



Omisión de autenticación en impresoras HP LaserJet Pro

Una investigación interna de HP ha reportado una vulnerabilidad de severidad alta, que afecta a dispositivos de impresión de la serie LaserJet Pro.

Avisos técnicos - Hasta el 3 de agosto

Vulnerabilidad RCE en ssh-agent de OpenSSH

El equipo Qualys Threat Research Unit (TRU) ha reportado una vulnerabilidad de severidad alta que podría permitir a un atacante remoto ejecutar comandos arbitrarios a través del ssh-agent de OpenSSH.

Avisos técnicos - Hasta el 3 de agosto

Vulnerabilidad zero-day en Apple

Apple ha publicado diversos avisos de seguridad, en los que se aborda una vulnerabilidad, cuyo identificador es CVE-2023-38606, que afecta a versiones de los sistemas operativos iOS, iPadOS, macOS, watchOS y tvOS. El fallo se debe a errores en el kernel que, a través de aplicaciones malintencionadas, pueden modificar su estado y no tiene asignada una puntuación de acuerdo con la escala CVSSv3, pero ha sido calificada por el fabricante como de tipo zero-day, por lo tanto, se les asigna una severidad crítica.

Avisos técnicos - Hasta el 3 de agosto

Vulnerabilidad de acceso remoto no autenticado en Ivanti Endpoint Manager Mobile (EPMM)

Ivanti ha informado de una vulnerabilidad en Ivanti Endpoint Manager Mobile (EPMM), anteriormente conocido como MobileIron Core, que permitiría a un usuario remoto no autorizado acceder a información personal de usuarios, o realizar cambios en el servidor, a través del acceso no autenticado a rutas API específicas.

Avisos técnicos - Hasta el 3 de agosto

[Actualización 02/08/2023] Vulnerabilidad de acceso remoto no autenticado en Ivanti Endpoint Manager Mobile (EPMM)

Ivanti ha informado de una vulnerabilidad en Ivanti Endpoint Manager Mobile (EPMM), anteriormente conocido como MobileIron Core, que permitiría a un usuario remoto no autorizado acceder a información personal de usuarios, o realizar cambios en el servidor, a través del acceso no autenticado a rutas API específicas.

Avisos técnicos - Hasta el 3 de agosto

Vulnerabilidad crítica en Ivanti Endpoint Manager Mobile

Ivanti ha publicado un aviso de seguridad donde se trata una vulnerabilidad de severidad crítica cuyo identificador es CVE-2023-35078. Este error permite que un actor remoto no autorizado, con acceso a Internet, acceda potencialmente a la información de identificación personal de los usuarios y realice cambios limitados en el servidor. Se conoce que esta vulnerabilidad ha sido explotada recientemente suponiendo una amenaza de alta gravedad para la confidencialidad, integridad y disponibilidad de los sistemas.

Avisos técnicos - Hasta el 3 de agosto

Múltiples vulnerabilidades en productos de HPE Aruba

HPE Aruba ha informado de varias vulnerabilidades en puntos de acceso que ejecuten InstantOS y ArubaOS 10. La explotación de estas vulnerabilidades podría permitir a un atacante realizar ejecuciones arbitrarias de código por desbordamientos de búfer, o fugas de información.

Avisos técnicos - Hasta el 3 de agosto

Vulnerabilidades en productos de Qnap

Qnap ha emitido dos avisos de seguridad referentes a vulnerabilidades identificadas como CVE-2022-27595 y CVE-2022-27600. El primer fallo que cuenta con una severidad alta, de ser explotado, puede permitir la ejecución de código, lo que supone una amenaza significativa para la confidencialidad, integridad y disponibilidad de los sistemas. En cuanto al segundo, de severidad media, su explotación puede conllevar condiciones de denegación de servicio, afectando especialmente a la disponibilidad de los sistemas.

Avisos técnicos - Hasta el 3 de agosto

Escritura remota de archivos arbitrarios en Ivanti EPMM

Mnemonic ha identificado una vulnerabilidad, de severidad alta, que afecta a Ivanti Endpoint Manager Mobile (EPMM), cuya explotación podría permitir la ejecución de comandos del sistema operativo.

Avisos técnicos - Hasta el 3 de agosto

Actualización de seguridad de Apple-Julio 2023

A lo largo del mes de julio, Apple ha publicado 13 actualizaciones de seguridad en las que se corrigen 53 fallos que afectan a los sistemas operativos iOS, iPadOS, macOS Ventura, Big Sur y Monterey, tvOS, watchOS y al navegador Safari. También se aportan actualizaciones Rapid Security Responses usadas para mejorar la seguridad entre actualizaciones de software.

Avisos técnicos - Hasta el 3 de agosto

Actualización de seguridad de Oracle-Julio 2023

El 18 de julio de 2023 Oracle publicó su boletín trimestral de actualizaciones de seguridad en el que se aportan 508 correcciones a vulnerabilidades para una amplia gama de productos, dentro de las cuales, 115 son susceptibles de una explotación remota, de forma que, pueden ser explotadas por un atacante para comprometer la integridad, confidencialidad y disponibilidad de los sistemas afectados, lo que podría resultar en una pérdida de datos y una interrupción de los servicios.

Avisos técnicos - Hasta el 3 de agosto

Vulnerabilidad en Ivanti Endpoint Manager Mobile (Core)

Ivanti ha publicado la actualización de un aviso de seguridad donde se trata la vulnerabilidad CVE-2023-35081, de severidad alta, que puede ser explotada en conjunción con la recientemente tratada CVE-2023-35078. El error permite que se realicen escrituras arbitrarias de archivos en el servidor EPMM y, de ser explotado, supondría una amenaza de alta gravedad para la confidencialidad, integridad y disponibilidad de los sistemas.

Avisos técnicos - Hasta el 3 de agosto

Vulnerabilidad de inyección SQL en ConacWin de Setelsa Security

INCIBE ha coordinado la publicación de una vulnerabilidad que afecta a ConacWin de Setelsa Security, una plataforma de control de acceso, la cual ha sido descubierta por David Cámara Galindo, de Telefónica Tech.

Avisos técnicos - Hasta el 3 de agosto

Vulnerabilidad de Cross-Site Scripting (XSS) en WideStand CMS de Acilia

INCIBE ha coordinado la publicación de una vulnerabilidad que afecta a WideStand CMS, una solución CMS profesional desarrollada por Acilia y basado en el framework Symfony, la cual ha sido descubierta por Ángel Heredia Pérez, de Telefónica Tech.

Avisos técnicos - Hasta el 3 de agosto

Cross Site Request Forgery en EasyVista

INCIBE ha coordinado la publicación de 1 vulnerabilidad que afecta a EasyVista 2016.1.305.2, la cual ha sido descubierta por Albert Sánchez Miñano.

Avisos técnicos - Hasta el 3 de agosto

Vulnerabilidades en Mozilla Firefox, Firefox ESR y Thunderbird

Mozilla, popular navegador de código abierto desarrollado para distintas plataformas, ha publicado 3 avisos de seguridad, 2023-29, 2023-30 y 2023-31 para corregir una serie de vulnerabilidades en sus navegadores web Firefox, Firefox ESR y Thunderbird, el cliente de correo electrónico desarrollado por la compañía.

Avisos técnicos - Hasta el 3 de agosto

Vulnerabilidad de acceso remoto no autenticado en Ivanti MobileIron Core

Stephen Fewer, investigador de Rapid7, ha reportado una vulnerabilidad crítica en Ivanti EPMM, cuya explotación podría permitir a un atacante, no autenticado, acceder a la API.

Avisos técnicos - Hasta el 3 de agosto

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 17 vulnerabilidades, de las cuales 9 cuentan con una severidad alta, cuyos identificadores son CVE-2023-4068, CVE-2023-4069, CVE-2023-4070, CVE-2023-4071, CVE-2023-4072, CVE-2023-4073, CVE-2023-4074, CVE-2023-4075 y CVE-2023-4076. Estos fallos, de ser explotados, conducen a condiciones de confusión de tipos, desbordamiento de búfer del heap, lectura y escritura fuera de límites y Use-After-Free.

Avisos técnicos - Hasta el 3 de agosto

Escalada de privilegios en dispositivos HP y Samsung

HeeChan Kim (@heegong123), investigador de TeamH4C, ha reportado una vulnerabilidad de severidad alta que afecta a múltiples impresoras de HP y Samsung, cuya explotación podría permitir una escalada de privilegios.

Avisos técnicos - Hasta el 3 de agosto