Boletín de Ciberseguridad N°75

Fecha de publicación: 26/02/2024

Mes de Febrero

23/01/2024 – 26/02/2024

Datasec

BOLETÍN DE CIBERSEGURIDAD

Indice

Introducción

Por medio de este boletín informativo estaremos destacando de forma quincenal, las noticias más relevantes en el ámbito de la ciberseguridad a nivel regional e internacional.

Las principales categorías de información son: vulnerabilidades tecnológicas, fraudes activos, amenazas por medios informáticos nuevos, así como recomendaciones específicas de prevención. La publicación de dichas noticias dependerá de la importancia y calidad informativa de las mismas.

A su vez se incluyen referencias técnicas y de gestión a los efectos de reducir los riesgos con anticipación y adecuada planificación.

En esta segunda quincena del mes de febrero se destacan 5 noticias de relevancia: 3 sobre vulnerabilidades tecnológicas, y 2 de prevención.

Aquellas noticias a tener especial recaudo son las siguientes:

Se detalla la reciente vulnerabilidad de los atajos de Apple

Han surgido detalles sobre una falla de seguridad de alta gravedad ahora parcheada en la aplicación Atajos de Apple que podría permitir un atajo para acceder a información confidencial en el dispositivo sin el consentimiento de los usuarios.

Akira Ransomware explota la vulnerabilidad de Cisco ASA/FTD

CISA agregó el jueves una falla de seguridad ahora parcheada que afecta el software Cisco Adaptive Security Appliance (ASA) y Firepower Threat Defense (FTD) a su catálogo de vulnerabilidades conocidas explotadas (KEV), luego de informes de que está siendo probablemente explotado en ataques de ransomware Akira.

Anuncios maliciosos de Google engañan a los usuarios de WinSCP

CISA agregó el lunes una falla de seguridad de gravedad media que afecta al software de correo electrónico Roundcube a su catálogo de vulnerabilidades explotadas conocidas (KEV), basándose en evidencia de explotación activa.

Vulnerabilidad Crítica

	Se detalla la reciente vulnerabilidad de los atajos de Apple	CRÍTICO

Descripción

Han surgido detalles sobre una falla de seguridad de alta gravedad ahora parcheada en la aplicación Atajos de Apple que podría permitir un atajo para acceder a información confidencial en el dispositivo sin el consentimiento de los usuarios.

Estado

Apple solucionó la vulnerabilidad, rastreada como CVE-2024-23204 (puntuación CVSS: 7,5), el 22 de enero de 2024, con el lanzamiento de iOS 17.3, iPadOS 17.3, macOS Sonoma 14.3.

Específicamente, la falla tiene su origen en una acción de acceso directo llamada "Expandir URL", que es capaz de expandir y limpiar URL que se han acortado usando un servicio de acortamiento de URL como t.co o bit.ly, al mismo tiempo que elimina los parámetros de seguimiento UTM.

Los datos exfiltrados luego se capturan y guardan como una imagen por parte del atacante utilizando una aplicación Flask, allanando el camino para una explotación posterior.

Remediación / Referencias

Se recomienda a todos los usuarios de Apple, que instalen la nueva versión.

Por más información acceder a:

https://nvd.nist.gov/vuln/detail/CVE-2024-23204

Vulnerabilidades de Wi-Fi exponen los dispositivos Android y Linux

CRÍTICO

Descripción

Se han identificado dos fallas de omisión de autenticación en el software Wi-Fi de código abierto que se encuentran en dispositivos Android, Linux y ChromeOS que podrían engañar a los usuarios para que se unan a un clon malicioso de una red legítima o permitir que un atacante se una a una red confiable sin una contraseña.

Estado

Las vulnerabilidades, rastreadas como CVE-2023-52160 y CVE-2023-52161, se descubrieron luego de una evaluación de seguridad de wpa_supplicant y iNet Wireless Daemon (IWD) de Intel, respectivamente.

CVE-2023-52161, en particular, permite que un adversario obtenga acceso no autorizado a una red Wi-Fi protegida, exponiendo a los usuarios y dispositivos existentes a posibles ataques como infecciones de malware, robo de datos y compromiso del correo electrónico empresarial (BEC). Afecta a las versiones 2.12 y anteriores de IWD.

Por otro lado, CVE-2023-52160 afecta a las versiones 2.10 y anteriores de wpa_supplicant. También es la más apremiante de las dos fallas debido al hecho de que es el software predeterminado utilizado en dispositivos Android para manejar solicitudes de inicio de sesión en redes inalámbricas.

Remediación / Referencias

Es fundamental que los usuarios de Android configuren manualmente el certificado CA de cualquier red empresarial guardada para evitar el ataque.

Por mayor información acceder a:

https://nvd.nist.gov/vuln/detail/CVE-2023-52160

Akira Ransomware explota la vulnerabilidad de Cisco ASA/FTD

CRÍTICO

Descripción

CISA agregó el jueves una falla de seguridad ahora parcheada que afecta el software Cisco Adaptive Security Appliance (ASA) y Firepower Threat Defense (FTD) a su catálogo de vulnerabilidades conocidas explotadas (KEV), luego de informes de que está siendo probablemente explotado en ataques de ransomware Akira.

Estado

La vulnerabilidad en cuestión es CVE-2020-3259 (puntuación CVSS: 7,5), un problema de divulgación de información de alta gravedad que podría permitir a un atacante recuperar el contenido de la memoria de un dispositivo afectado. Cisco lo parchó como parte de las actualizaciones publicadas en mayo de 2020.

CVE-2020-3259 está lejos de ser el único defecto que se puede explotar para distribuir ransomware. A principios de este mes, Arctic Wolf Labs reveló el abuso de CVE-2023-22527 (una deficiencia descubierta recientemente en Atlassian Confluence Data Center y Confluence Server) para implementar el ransomware C3RB3R, así como mineros de criptomonedas y troyanos de acceso remoto.

El esquema de ransomware como servicio (RaaS), al igual que Hive, comprometió a más de 1000 víctimas en todo el mundo, generando al menos 300 millones de dólares en ganancias ilícitas desde su aparición a finales de 2021. Fue interrumpido en diciembre de 2023 luego de una operación coordinada internacional.

Remediación / Referencias

Se pidió una mayor supervisión de las prácticas recomendadas para abordar el ransomware, específicamente para organizaciones de sectores críticos de fabricación, energía, atención médica y salud pública, y sistemas de transporte.

Por mayor información acceder a:

https://nvd.nist.gov/vuln/detail/CVE-2020-3259

Prevención

	Anuncios maliciosos de Google engañan a los usuarios de WinSCP	PREVENCIÓN

Descripción

CISA agregó el lunes una falla de seguridad de gravedad media que afecta al software de correo electrónico Roundcube a su catálogo de vulnerabilidades explotadas conocidas (KEV), basándose en evidencia de explotación activa.

Estado

El problema, rastreado como CVE-2023-43770 (puntuación CVSS: 6,1), se relaciona con una falla de secuencias de comandos entre sitios (XSS) que surge del manejo de enlaces en mensajes de texto sin formato.

Según una descripción del error en la Base de datos nacional de vulnerabilidades (NVD) del NIST, la vulnerabilidad afecta a las versiones de Roundcube anteriores a 1.4.14, 1.5.x anteriores a 1.5.4 y 1.6.x anteriores a 1.6.3.

Actualmente no se sabe cómo se está explotando la vulnerabilidad en la naturaleza, pero las fallas en el cliente de correo electrónico basado en la web han sido utilizadas como arma por actores de amenazas vinculados a Rusia como APT28 y Winter Vivern durante el año pasado.

Remediación / Referencias

Se recibió el mandato de aplicar correcciones proporcionadas por los proveedores antes del 4 de marzo de 2024 para proteger sus redes contra posibles amenazas.

Por mayor información acceder a:

https://nvd.nist.gov/vuln/detail/CVE-2023-43770

	Microsoft lanza parches para 73 fallas	PREVENCIÓN

Descripción

Microsoft ha lanzado parches para abordar 73 fallas de seguridad que abarcan su línea de software como parte de sus actualizaciones del martes de parches para febrero de 2024, incluidos dos días cero que han sido objeto de explotación activa.

Estado

De las 73 vulnerabilidades, 5 están clasificadas como críticas, 65 como importantes y tres como moderadas en gravedad. Esto se suma a las 24 fallas que se han solucionado en el navegador Edge basado en Chromium desde el lanzamiento de las actualizaciones del martes de parches de enero de 2024.

Las dos fallas que figuran como bajo ataque activo en el momento del lanzamiento se encuentran a continuación:

- CVE-2024-21351 (puntuación CVSS: 7,6): vulnerabilidad de omisión de la función de seguridad SmartScreen de Windows
- CVE-2024-21412 (puntuación CVSS: 8,1): vulnerabilidad de omisión de la función de seguridad de archivos de acceso directo a Internet

La explotación exitosa de la falla podría permitir a un atacante eludir las protecciones de SmartScreen y ejecutar código arbitrario. Sin embargo, para que el ataque funcione, el actor de la amenaza debe enviar al usuario un archivo malicioso y convencerlo de que lo abra.

CVE-2024-21412, de manera similar, permite a un atacante no autenticado eludir los controles de seguridad mostrados enviando un archivo especialmente diseñado a un usuario objetivo.

Microsoft también corrigió cinco fallas críticas:

- CVE-2024-20684 (puntuación CVSS: 6,5): vulnerabilidad de denegación de servicio de Hyper-V en Windows.
- CVE-2024-21357 (puntuación CVSS: 7,5): vulnerabilidad de ejecución remota de código de multidifusión general pragmática (PGM) de Windows.
- CVE-2024-21380 (puntuación CVSS: 8.0) - Vulnerabilidad de divulgación de información de Microsoft Dynamics Business Central/NAV.
- CVE-2024-21410 (puntuación CVSS: 9,8): vulnerabilidad de elevación de privilegios en Microsoft Exchange Server.

- CVE-2024-21413 (puntuación CVSS: 9,8): vulnerabilidad de ejecución remota de código en Microsoft Outlook.

Remediación / Referencias

Además de Microsoft, otros proveedores también han publicado actualizaciones de seguridad durante las últimas semanas para rectificar varias vulnerabilidades, entre ellas:

- Adobe
- AMD
- Androide
- Brazo
- ASUS
- Atos
- Canon
- cisco
- Dell
- drupal
- ExpressVPN
- F5
- Fortinet
- GitLab
- Google Chrome
- Nube de Google
- Energía Hitachi
- caballos de fuerza
- IBM
- Intel
- ISC ENLACE 9
- Ivanti
- JetBrains TeamCity
- Redes de enebro
- lenovo
- Distribuciones de Linux Debian, Oracle Linux, Red Hat, SUSE y Ubuntu
- Mastodonte
- MediaTek
- Mitsubishi Electrico
- Mozilla Firefox, Firefox ESR y Thunderbird
- Nvidia
- PowerDNS
- QNAP (más detalles sobre CVE-2023-47218 y CVE-2023-50358)
- Qualcomm
- Automatización Rockwell
- Samsung
- SAVIA
- Schneider Electric
- siemens

- Vientos solares
- SonicWall
- Marco de primavera
- Sinología
- Veeam
- Veritas
- VMware
- WordPress
- Ampliar y
- Zyxel

Toda la información aquí:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-21351

Conclusiones

En un entorno de trabajo remoto en constante evolución, la seguridad de las conexiones sigue siendo una prioridad fundamental.
Mantenernos a salvo de posibles amenazas es crucial. La actualización constante y la configuración segura de estos componentes son esenciales para mitigar riesgos. Además, es valioso contar con herramientas que evalúen la salud de los dispositivos remotos, asegurando que los sistemas operativos estén al día y los controles de seguridad estén activos.

Estas medidas no solo previenen posibles abusos o compromisos, sino que también fortalecen la ciberseguridad en general. La implementación de soluciones como Fortinet's FortiClient Health Check o Duo Security Device Health, entre otras, puede marcar la diferencia en la postura de seguridad de una organización.

La autenticación de doble factor es un pilar en la protección de accesos remotos, reduciendo significativamente la probabilidad de incidentes de seguridad.
En resumen, la seguridad en las conexiones remotas es un compromiso continuo. Al mantenerse actualizados y aplicar configuraciones seguras, las organizaciones pueden protegerse contra amenazas y garantizar un entorno de trabajo remoto seguro y confiable.

En Datasec, seguimos dedicados a salvaguardar la seguridad de nuestros clientes, socios y colaboradores, y alentamos a todos a mantener un enfoque constante en la seguridad cibernética.

¡Sigamos trabajando juntos para mantenernos protegidos!