Boletín de Ciberseguridad N°79

Fecha de publicación: 08/05/2024

16/04/2024 – 08/05/2024

Datasec

BOLETÍN DE CIBERSEGURIDAD

Indice

Introducción

En esta nueva entrega del boletín informativo de ciberseguridad, compartimos un resumen de las noticias más relevantes a nivel regional e internacional que afectan la seguridad de la información.

A nivel internacional, el 2 de mayo se celebró el Día Mundial de la Contraseña con el fin de concientizar sobre la importancia de la utilización de contraseñas robustas, únicas y que no sean compartidas con nadie más que el usuario. En este sentido, desde Datasec motivamos además a tomar medidas que se complementen con una contraseña de estas características, como ser: activar la autenticación en dos pasos siempre que se pueda, mantener un sistema operativo actualizado y con antimalware, realizar respaldos de seguridad regulares y tener especial precaución al guardar contraseñas en navegadores.

Los invitamos a continuación a conocer algunas de las vulnerabilidades destacadas en esta última quincena, así como medidas de prevención y novedades generales en el ámbito de la ciberseguridad.

Vulnerabilidad Crítica

GitLab	Gitlab: toma de control de cuenta a través de reinicio de contraseña sin interacciones del usuario	CRÍTICO

Descripción

Se ha descubierto un problema en GitLab CE/EE que afecta a todas las siguientes versiones:

16.1 a 16.1.5
16.2 a 16.2.8
16.3 a 16.3.6
16.4 a 16.4.4
16.5 a 16.5.5
16.6 a 16.6.3
16.7 a 16.7.1

En estos casos, los correos electrónicos de reinicio de contraseña de la cuenta de usuario podrían ser entregados a una dirección de correo electrónico no verificada.

Estado: Crítico

Actualmente se encuentra mitigado en la última versión y se le ha asignado el CVE-2023-7028.

Remediación / Referencias

Se recomienda que todas las instalaciones que estén ejecutando una versión afectada por los problemas descritos anteriormente sean actualizadas a la última versión lo antes posible. Para ello, existe un parche más reciente que incluye correcciones adicionales para un problema de migración de base de datos descubierto recientemente. Se recomienda actualizar a la versión 16.7.3, 16.6.5, 16.5.7 o una versión más nueva para prevenir el problema de migración.

Además, se recomienda tomar las siguientes medidas:
1- Actualizar a la última versión
2- Habilitar la autenticación de dos factores (2FA) para todas las cuentas de GitLab.
3- Modificar todas las credenciales almacenadas en GitLab:

- Todas las credenciales, incluyendo las contraseñas de la cuenta de GitLab
- Tokens de API
- Cualquier certificado
- Otros secretos

Por mayor información acceder a:

https://about.gitlab.com/releases/2024/01/11/critical-security-release-gitlab-16-7-2-released/

CISCO	ArcaneDoor: explotan dos vulnerabilidades Zero-Day de Cisco ASA	CRÍTICO

Descripción

Una nueva campaña de malware aprovechó dos vulnerabilidades Zero-Day en los equipos de red de Cisco Adaptive Security Appliances (ASA) para entregar malware personalizado y facilitar la recopilación encubierta de datos.

"UAT4356 implementó dos puertas traseras como componentes de esta campaña, 'Line Runner' y 'Line Dancer', que se usaron colectivamente para llevar a cabo acciones maliciosas en el objetivo, que incluyeron modificación de configuración, reconocimiento, captura/exfiltración de tráfico de red y potencialmente movimiento lateral", dijo Talos.

- CVE-2024-20353 (puntuación CVSS: 8,6): vulnerabilidad de denegación de servicio de servicios web del software Cisco Adaptive Security Appliance y Firepower Threat Defense
- CVE-2024-20359 (puntuación CVSS: 6,0): vulnerabilidad de ejecución persistente de código local del software Cisco Adaptive Security Appliance y Firepower Threat Defense

Si bien la segunda falla permite que un atacante local ejecute código arbitrario con privilegios de nivel *root*, se requieren privilegios de nivel de administrador para explotarlo. Junto con CVE-2024-20353 y CVE-2024-20359, en pruebas internas se descubrió una falla de inyección de comandos en el mismo dispositivo (CVE-2024-20358, puntuación CVSS: 6,0). Actualmente se desconoce la vía de acceso inicial exacta utilizada para violar los dispositivos, aunque se dice que UAT4356 comenzó los preparativos para ello ya en julio de 2023.

Estado: crítico

Remediación:

Como primera medida para que los datos entren y salgan de la red, estos dispositivos deben ser parcheados de manera rutinaria y rápida; usar versiones y configuraciones de hardware y software actualizadas; y ser monitoreados de cerca desde una perspectiva de seguridad. Estos dispositivos permiten a un actor ingresar directamente a una organización, redirigir o modificar el tráfico y monitorear las comunicaciones de la red.

Por mayor información acceder a:

https://blog.segu-info.com.ar/2024/04/explotan-dos-vulnerabilidades-zero-day.html

Prevención

	Google Chrome: nueva criptografía postcuántica v124 puede romper conexiones TLS	PREVENCIÓN

Descripción:

Algunos usuarios de Google Chrome informan que han tenido problemas para conectarse a sitios web, servidores y firewalls después del lanzamiento de Chrome 124 la semana pasada con el nuevo mecanismo de encapsulación X25519Kyber768 resistente a ataques cuánticos y habilitado de forma predeterminada.

Google comenzó a probar el mecanismo de encapsulación de claves TLS seguro poscuántico en agosto y ahora lo ha habilitado en la última versión de Chrome para todos los usuarios. La nueva versión utiliza el algoritmo de acuerdo de clave Kyber768 quantum-resistant para conexiones TLS 1.3 y QUIC para proteger el tráfico TLS de Chrome contra el criptoanálisis cuántico.

Esto protege el tráfico de los usuarios de los ataques llamados "almacenar ahora y descifrar después" (Store Now, Decrypt Later - SNDL), en los que una futura computadora cuántica podría descifrar el tráfico cifrado registrado hoy.

Los ataques de "almacenar ahora, descifrar más tarde" son cuando los atacantes recopilan datos cifrados y los almacenan para el futuro, cuando puedan haber nuevos métodos de descifrado, como el uso de computadoras cuánticas o claves de cifrado disponibles.

Para protegerse contra futuros ataques, las empresas ya han comenzado a agregar cifrado resistente a ataques post-cuánticos a su pila de red para evitar que este tipo de estrategias de descifrado funcionen en el futuro. Algunas empresas que ya han introducido algoritmos resistentes a los cuánticos son Apple, Signal, y Google.

Por mayor información acceder a:
https://blog.segu-info.com.ar/2024/04/nueva-criptografia-poscuantica-de.html

Novedades

wazuh.	Datasec y Wazuh refuerzan su alianza estratégica para proteger entornos digitales	NOVEDADES

Nos complace anunciar que hemos renovado nuestra colaboración con Wazuh, el referente en seguridad de código abierto, fortaleciendo aún más nuestra alianza de nivel Oro a nivel Platino. Esta renovación de nuestra asociación refuerza nuestro compromiso con la excelencia en ciberseguridad.

En Datasec, nos esforzamos por proporcionar soluciones de ciberseguridad de primer nivel y nuestra colaboración con Wazuh es fundamental para lograr este objetivo. Wazuh es reconocido como líder en Seguridad de la Información y Gestión de Eventos (SIEM) y Detección y Respuesta Extendida (XDR) de código abierto y su integración en nuestro ecosistema de seguridad nos permite ofrecer a nuestros clientes soluciones más completas y efectivas.

¿Por qué Wazuh?

"Nuestra decisión de elegir Wazuh fue impulsada por sus sólidas capacidades, las cuales se alinean perfectamente con nuestra misión de proteger los activos informáticos de nuestros clientes en diversos entornos", expresó nuestro Socio Director Reynaldo de la Fuente. La flexibilidad de la plataforma de código abierto de Wazuh permite adaptar las medidas de seguridad a las necesidades específicas de cada cliente, mientras que su comunidad activa y actualizaciones continuas garantizan que siempre estén a la vanguardia de las innovaciones en ciberseguridad.

Es así que Wazuh representa una herramienta fundamental para nuestro servicio de monitoreo 24/7 (SOC) que proporciona un análisis continuo de amenazas, detección y respuesta para prevenir y mitigar incidentes en materia de ciberseguridad. Este tipo de monitoreo representa un componente crítico de cualquier estrategia integral de ciberseguridad en una organización.

Nuestros servicios de supervisión continua son llevados a cabo por un equipo especializado que detecta y responde a amenazas en tiempo real 24/7.

Estamos emocionados de continuar trabajando estrechamente con Wazuh para brindar a nuestros clientes las mejores herramientas y servicios para proteger sus activos digitales y enfrentar los desafíos de seguridad cibernética de manera efectiva. Esta colaboración renovada subraya nuestro compromiso con la innovación, la calidad y la seguridad en todos los aspectos de nuestro trabajo.

Nueva legislación en Reino Unido para fabricantes de dispositivos inteligentes sobre medidas de seguridad

NOVEDADES

A partir del 29 de abril de este año, los fabricantes de dispositivos “inteligentes” deben garantizar que todos sus dispositivos cumplan con los requisitos básicos de ciberseguridad, según la Ley de Seguridad de Productos e Infraestructura de Telecomunicaciones en Reino Unido.

Estas medidas establecen que el fabricante:

- No debe suministrar dispositivos que utilicen contraseñas predeterminadas, que puedan descubrirse fácilmente en línea y ser compartidas.
- Debe proporcionar un punto de contacto para informar sobre problemas de seguridad que, si se ignoran, podrían hacer que los dispositivos sean intervenidos por ciberdelincuentes
- Debe indicar la duración mínima durante la cual el dispositivo recibirá actualizaciones de seguridad importantes. Cuando las actualizaciones ya no se proporcionan, los dispositivos son más fáciles de hackear o pueden dejar de funcionar como se diseñaron.

La ley se aplica a cualquier dispositivo inteligente que se conecte a internet o a una red doméstica, tales como altavoces, televisores, cámaras de seguridad, tablets, teléfonos, consolas de juegos, electrodomésticos inteligentes, entre otros.

Si bien la mayoría de los dispositivos se fabrican fuera de Reino Unido, la ley también actúa sobre todas las importaciones y ventas para el mercado de Reino Unido.

Por más información acceder a:
https://www.ncsc.gov.uk/blog-post/smart-devices-law#:~:text=From%2029%20April%202024%2C%20manufacturers,ongoing%20protection%20against%20cyber%20attacks

Conclusiones

Considerando el avance y sofisticación de los ataques cibernéticos, continúa siendo una tarea y responsabilidad constante de los usuarios y organizaciones, mantener sus equipos y sistemas resguardados con todas las medidas que estén a su alcance.

La autenticación en dos pasos sigue siendo un mecanismo fuerte de prevención, reduciendo la posibilidad de acceso a la información en caso de contraseñas vulneradas o fugadas.

A su vez, la constante actualización y la aplicación de configuraciones seguras deben ser medidas recurrentes e instaladas en cualquier organización con el fin de proteger su información.

Desde Datasec, seguimos trabajando en nuestras distintas áreas de consultoría, SOC, Hacking ético y capacitación, con el fin de seguir brindando las mejores y más actualizadas soluciones en ciberseguridad para empresas y organizaciones de la región.