ALERTA

TLP:CLEAR

Principales vulnerabilidades explotadas en 2023

COLCERT AL-1511-056

Recientemente, la Agencia de Seguridad Cibernética e Infraestructura de EE. UU. (CISA) emitió una advertencia sobre las vulnerabilidades cibernéticas más comunes que han sido explotadas en 2023. Destacaron un aumento significativo en el uso de vulnerabilidades de día cero por parte de actores maliciosos. Esta tendencia es preocupante, ya que también se aplica a la realidad cibernética en Colombia, donde las infraestructuras críticas y los sistemas empresariales son blancos para los atacantes.

Top de vulnerabilidades

Esta tabla resume las 15 vulnerabilidades más explotadas en 2023. La gestión de éstas es crucial porque permite identificar y priorizar riesgos, mitigar amenazas inmediatas y mejorar la postura de seguridad. No remediarlas puede resultar en ataques exitosos que comprometan sistemas críticos, provoquen pérdida de información y afecten la continuidad de las operaciones.

CVE	Descripción	Impacto
CVE-2023-3519	Afecta a Citrix NetScaler ADC y Gateway. Permite a un usuario no autenticado causar un desbordamiento de búfer.	Ejecución remota de código.
CVE-2023-4966	Afecta a Citrix NetScaler ADC y Gateway. Permite la filtración de tokens de sesión.	Exposición de información sensible.
CVE-2023-20198	Afecta a Cisco IOS XE Web UI. Permite a usuarios no autorizados crear usuarios locales.	Acceso no autorizado a sistemas.
CVE-2023-20273	Afecta a Cisco IOS XE. Permite la escalada de privilegios a raíz tras la creación de un usuario local.	Acceso completo al sistema.
CVE-2023-27997	Afecta a Fortinet FortiOS y FortiProxy SSL-VPN. Permite ejecutar código arbitrario mediante solicitudes específicas.	Ejecución remota de código.
CVE-2023-34362	Afecta a Progress MOVEit Transfer. Permite abuso de una vulnerabilidad de inyección SQL para obtener un token API.	Ejecución remota de código y acceso no autorizado.
CVE-2023-22515	Afecta a Atlassian Confluence Data Center y Server. Problema de validación de entrada que permite ejecución de código.	Ejecución remota de código mediante modificación de objetos Java en tiempo de ejecución.
CVE-2021-44228	Conocida como Log4Shell, afecta a la biblioteca Log4j de Apache. Permite la ejecución arbitraria de código.	Control total del sistema afectado, robo de información, ransomware, etc.
CVE-2023-2868	Afecta al Barracuda Networks ESG Appliance. Permite la ejecución remota de comandos del sistema no autorizados.	Acceso no autorizado y control del sistema afectado.
CVE-2022-47966	Afecta a productos que usan Zoho ManageEngine. Permite ejecución arbitraria de código mediante SAML malicioso.	Ejecución remota de código sin autenticación previa.
CVE-2023-27350	Afecta a PaperCut MF/NG. Permite encadenar vulnerabilidades para ejecutar código sin autenticación.	Ejecución remota de código y acceso no autorizado.
CVE-2020-1472	Afecta a Microsoft Netlogon. Permite escalada de privilegios mediante conexiones inseguras a controladores de dominio.	Escalada no autorizada a privilegios elevados dentro del dominio.
CVE-2023-42793	Afecta a JetBrains TeamCity servidores. Permite bypass de autenticación y ejecución remota de código.	Acceso no autorizado y ejecución remota en servidores vulnerables.
CVE-2023-23397	Afecta a Microsoft Office Outlook. Permite elevación de privilegios mediante correos electrónicos maliciosos.	Acceso elevado sin interacción del usuario, comprometiendo la seguridad del sistema Outlook.
CVE-2023-49103	Afecta a ownCloud graphapi. Permite divulgación no autorizada de información sensible como contraseñas y claves.	Exposición grave de datos confidenciales sin autenticación previa.

COLCERT

ALERTA

Principales vulnerabilidades explotadas en 2023

COLCERT AL-1511-056

Potenciales Consecuencias para Colombia

- Aumento en ataques cibernéticos: la exploración de vulnerabilidades como CVE-2023-3519 y CVE-2023-20198 lleva, respectivamente, a accesos no autorizados y control total de sistemas críticos. Esto podría llevar a la paralización de servicios básicos de sectores críticos.
- Robo de información sensible: las vulnerabilidades, como CVE-2023-34362, permiten a los atacantes obtener tokens de acceso y ejecutar código remotamente. Los daños para empresas y ciudadanos en caso de robo de información confidencial pueden ser crítica.
- Impacto económico: las empresas pueden sufrir pérdidas económicas considerables debido a la interrupción de las operaciones y la necesidad de invertir recursos en la mejora de la seguridad.

Recomendaciones para Mitigación

- Actualización rápida de sistemas: Se hace un llamado a todas las entidades y organizaciones a aplicar parches a sus sistemas operativos y aplicaciones, priorizando aquellas vulnerabilidades identificadas en esta alerta.
- Implementar las siguientes medidas de seguridad no solo ayudará a las organizaciones a proteger sus activos digitales, sino que también fomentará una cultura organizacional centrada en la ciberseguridad, esencial en el entorno digital actual.

Medida de Seguridad	Descripción
Capacitación y concienciación del personal	Realizar capacitaciones periódicas sobre ciberseguridad para todos los empleados, enfatizando políticas de seguridad y amenazas como el phishing.
Actualización de sistemas	Mantener todos los sistemas operativos y aplicaciones actualizados para cerrar vulnerabilidades que puedan ser explotadas por atacantes.
Implementación de controles de acceso	Establecer políticas estrictas de control de acceso, asegurando que solo el personal autorizado pueda acceder a información sensible. Utilizar autenticación multifactor (MFA).
Protección de redes	Utilizar herramientas como firewalls, mirosegmenetación y VPNs para proteger la red empresarial y controlar el acceso. Crear redes separadas para visitantes o dispositivos personales.
Copia de seguridad de datos	Realizar copias de seguridad regulares de toda la información crítica y asegurarse que estas copias estén almacenadas en un lugar seguro y accesible.
Desarrollo de políticas de seguridad	Diseñar e implementar políticas claras sobre el uso seguro de tecnología, incluyendo contraseñas robustas y la prohibición de abrir enlaces o descargar archivos sospechosos.
Monitoreo continuo	Establecer un sistema de monitoreo continuo para detectar comportamientos inusuales en la red que puedan indicar un ciberataque inminente.
Evaluaciones periódicas de riesgos	Realizar análisis regulares para identificar vulnerabilidades en los sistemas y ajustar las medidas de seguridad según sea necesario.
Protocolos de respuesta a incidentes	Desarrollar un protocolo claro para responder a incidentes cibernéticos, incluyendo pasos a seguir en caso de un ataque.

NIVEL DE RIESGO

ALTO

FUENTE:
https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-317a

COLCERT