Advertencia

Vulnerabilidades explotadas

COLCERT AD-20251020-029

TLP:CLEAR

El aviso emitido por CISA (Cybersecurity and Infrastructure Security Agency) el 14 de octubre de 2025 anuncia la **incorporación de cinco nuevas vulnerabilidades explotadas activamente** al catálogo **KEV** (por sus siglas en inglés, Known Exploited Vulnerabilities Catalog, es un catálogo oficial mantenido por la CISA que recopila todas las vulnerabilidades que ya han sido explotadas activamente en el mundo real por actores maliciosos), evidenciando un incremento sostenido en el aprovechamiento de fallas conocidas por actores de amenaza.

Este hecho refuerza la probabilidad alta de que sistemas sin parches continúen siendo objetivos prioritarios en campañas futuras, especialmente aquellos basados en **Windows** y herramientas de monitoreo como **Velociraptor**. De mantenerse la tendencia, se anticipa un aumento en incidentes orientados a escalación de privilegios y ejecución remota de código, con potencial impacto operacional y reputacional significativo. La anticipación estratégica exige fortalecer los procesos de gestión de vulnerabilidades y **priorizar la corrección de las CVE incluidas en el catálogo**, mitigando así la exposición ante amenazas de explotación recurrente.

NIVEL DE RIESGO

ALTO

Vulnerabilidades explotadas

CVE	Producto afectado	Score CVSS	Riesgo	Notas relevantes
CVE-2016-7836	SKYSEA Client View	**9.8 (Crítico)**	Permite autenticación no autorizada.	Aunque es antigua, sigue siendo explotada, lo que indica presencia de sistemas sin parches.
CVE-2025-6264	Rapid7 Velociraptor	**5.5 (Medio)**	Podría permitir escalación de privilegios o modificación no autorizada.	Importante para entornos de análisis forense o monitoreo donde se usa Velociraptor.
CVE-2025-24990	Microsoft Windows	**7.8 (Alto)**	Ejecución remota de código (RCE) o denegación de servicio.	Relacionada con componentes del *kernel* o manejo de memoria.
CVE-2025-47827	IGEL OS	**4.6 (Medio)**	Riesgo criptográfico: autenticación insegura o bypass de verificación.	Afecta entornos de escritorios virtuales.
CVE-2025-59230	Microsoft Windows	**7.8 (Alto)**	Escalación de privilegios locales.	Muy relevante para persistencia postexplotación.

Impacto para Colombia y la región

- **Principales sectores afectados**: gobierno, financiero, salud, educación, energía, TIC.
- **Riesgo alto**: el nivel de riesgo es alto debido a que las vulnerabilidades incluidas en el catálogo KEV presentan explotación activa confirmada, lo que incrementa la probabilidad de ataques dirigidos en entornos locales que utilicen sistemas Windows, plataformas de monitoreo o gestión de activos digitales. Además, la persistencia de sistemas sin parchear y la dependencia regional de tecnologías globales como Microsoft incrementan la superficie de exposición.
- **Posibles consecuencias**: compromiso de infraestructuras críticas, interrupción de servicios esenciales, captura o alteración de información confidencial, escalación de privilegios en redes corporativas y afectación reputacional para las organizaciones. En sectores como el financiero o salud, un ataque exitoso podría derivar en impactos regulatorios y pérdidas económicas significativas.

- **Implicaciones en seguridad digital:** estas vulnerabilidades subrayan la necesidad urgente de fortalecer la gestión de vulnerabilidades y los programas de actualización de software en las organizaciones de la región. Su explotación demuestra que los actores maliciosos continúan aprovechando fallas conocidas para mantener acceso y persistencia en redes vulnerables. La anticipación estratégica requiere monitoreo constante de los boletines KEV, priorización de parches y verificación de configuraciones seguras para mitigar riesgos en infraestructuras tecnológicas críticas.

Mitigaciones MITRE

MITIGACIÓN	CÓDIGO	RELEVANCIA
Actualizar software	**M1051**	La corrección oportuna (patching) elimina las fallas explotadas activamente, es la medida primaria contra CVE como las de Microsoft y productos con permisos por defecto. Para este aviso KEV, priorizar el despliegue de parches reduce la ventana de exposición.
Configuración de software segura	**M1054**	Ajustar configuraciones, deshabilitar funciones innecesarias, endurecer políticas, y habilitar controles de autenticación, mitiga vectores como "improper authentication" y claves expiradas.
Gestión de cuentas privilegiadas	**M1026**	Restringir, rotar y auditar cuentas privilegiadas limita el impacto de explotaciones que llevan a escalación de privilegios o persistencia (p. ej. CVE de Windows que permiten escalación). Implementar PAM reduce la capacidad del atacante de moverse y mantener control
Segmentación de red	**M1030**	Separar activos críticos y exponer servicios mínimos entre segmentos evita la expansión lateral tras una explotación inicial (importante si una máquina con Velociraptor o Windows es comprometida). La segmentación reduce el alcance y el impacto operativo de incidentes.

Soluciones y mitigaciones disponibles

- **CVE-2016-7836** (SKYSEA Client View): actualizar SKYSEA Client View a la versión 11.300.08h o superior, asegurándose de tener el patch que soluciona el fallo de autenticación en las conexiones TCP-al management console. Restringir el acceso de red al *management console*, permitiendo solo hosts de confianza mediante firewall, VPN o segmentación de red. Deshabilitar o desactivar servicios remotos innecesarios asociados al componente vulnerable, mientras se realiza la actualización. Verificar luego de la actualización que las pruebas funcionales pasen (incluyendo autenticación, acceso remoto) y que no queden puntos expuestos por configuración heredada.

- **CVE-2025-6264** (Rapid7 Velociraptor): actualizar Velociraptor a la versión 0.74.3 o superior, ya que esa versión corrige la vulnerabilidad del artefacto *Admin.Client.UpdateClientConfig*. Restringir los permisos del rol COLLECT_CLIENT para impedir que usuarios con ese rol accedan al artefacto vulnerable hasta que la actualización esté desplegada.

- **CVE-2025-24990** (Microsoft Windows): instalar inmediatamente la actualización acumulativa de Microsoft que elimina el driver Agere Modem (ltmdm64.sys) para corregir esta vulnerabilidad. Desactivar o remover dependencias de hardware que utilizan este *driver*, si existen, para mitigar exposición si el driver no se puede eliminar por completo. Verificar mediante inventario de sistemas (hardware + drivers) qué máquinas lo tienen instalado, incluso aquellas en desuso, para asegurar cobertura completa de remediación. Validar luego de aplicar el parche que el driver ya no se carga, monitorear logs de *kernel* o eventos del sistema para detectar intentos de llamadas al driver vulnerables.

- **CVE-2025-47827** (IGEL OS): actualizar IGEL OS a versiones 11 o superiores, ya que las versiones previas a la 11 están afectadas. Restringir el uso del módulo igel-flash-driver en dispositivos IGEL OS 10 hasta que esté actualizado o reemplazado, como medida temporal.

- **CVE-2025-59230** (Microsoft Windows): aplicar sin demora la actualización de seguridad publicada por Microsoft para corregir la vulnerabilidad en RASMAN. Restringir el acceso local al servicio *Remote Access Connection Manager* mediante políticas de control de acceso, de modo que solo usuarios autorizados puedan interaccionar con él. Implementar el principio de menor privilegio (least privilege) en cuentas de usuario locales, reduciendo permisos de usuarios que podrían interactuar con RASMAN. Monitorear los eventos de seguridad locales relacionados con elevación de privilegios o movimientos inusuales en procesos asociados a RASMAN, para detectar explotación temprana.

- Fortalecer los procesos de gestión de vulnerabilidades estableciendo un ciclo continuo de identificación, evaluación, priorización y remediación, que permita abordar de manera proactiva las fallas incluidas en el KEV y reducir la ventana de exposición frente a actores que aprovechan vulnerabilidades conocidas.

- Capacitar al personal técnico y de seguridad sobre la importancia del seguimiento del catálogo KEV y los boletines de CISA, fomentando la cultura de actualización temprana y la comprensión del riesgo operativo que representan las vulnerabilidades explotadas activamente.

- Reforzar las políticas de respaldo y recuperación ante incidentes, asegurando que los sistemas críticos tengan copias actualizadas y verificadas, de manera que un posible ataque derivado de estas vulnerabilidades no comprometa la continuidad operativa.

Fuentes

CISA, 14 octubre 2025, 14 octubre 2025, CISA Adds Five Known Exploited Vulnerabilities to Catalog, fuente oficial gubernamental.
https://www.cisa.gov/news-events/alerts/2025/10/14/cisa-adds-five-known-exploited-vulnerabilities-catalog
NVD, 2025, 14 octubre 2025, CVE-2025-59230 Detail, base de datos de vulnerabilidades.
https://nvd.nist.gov/vuln/detail/CVE-2025-59230
NVD, 2025, 05 junio 2025, CVE-2025-47827 Detail, base de datos de vulnerabilidades.
https://nvd.nist.gov/vuln/detail/CVE-2025-47827
NVD, 2025, 14 octubre 2025, CVE-2025-24990 Detail, base de datos de vulnerabilidades.
https://nvd.nist.gov/vuln/detail/CVE-2025-24990
NVD, 2025, 19 junio 2025, CVE-2025-6264 Detail, base de datos de vulnerabilidades.
https://nvd.nist.gov/vuln/detail/CVE-2025-6264
NVD, 2016, 09 junio 2017, CVE-2016-7836 Detail, base de datos de vulnerabilidades.
https://nvd.nist.gov/vuln/detail/cve-2016-7836
Microsoft Security Response Center, 2025, 14 octubre 2025, CVE-2025-59230 Update Guide, fuente oficial del proveedor.
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-59230