Alerta Id	0022
Fecha del reporte	2025/08/29
Entidad	Instituto de Evaluación Tecnológica en Salud IETS
Título	Reporte semanal de monitoreo y gestión de aplicaciones en endpoints
Herramienta de detección	FortiEDR
Tipo de alerta	Vulnerabilidad
Nivel de riesgo	Crítica

Introducción:

El presente informe tiene como objetivo documentar y analizar la actividad reciente de aplicaciones detectadas en los endpoints de la red institucional, utilizando la herramienta Fortinet EDR. El enfoque se centra en identificar comportamientos anómalos, evaluar el riesgo asociado a las aplicaciones observadas y proponer acciones correctivas o preventivas según el nivel de criticidad detectado.

Se ha revisado la sección Communication Control, donde se visualiza el tráfico generado por las aplicaciones ejecutadas en los dispositivos monitoreados. Este módulo permite aplicar políticas de control, identificar binarios no firmados, evaluar vulnerabilidades conocidas y tomar decisiones con base en la reputación del software detectado.

Este análisis se enmarca dentro de las tareas de ciberseguridad continua con el fin de garantizar la integridad, disponibilidad y confidencialidad de los activos tecnológicos de la organización.

Resumen ejecutivo:

Este reporte semanal presenta los hallazgos obtenidos durante el monitoreo de aplicaciones ejecutadas en los endpoints de la red, correspondientes al periodo **21 al 28 de agosto**. Se identificaron varias aplicaciones activas con distintos niveles de riesgo, incluyendo binarios no firmados, aplicaciones con vulnerabilidades críticas, y herramientas sin reputación registrada.

Aplicaciones destacadas:

Aplicación	Firma	Vendor	Reputación	Vulnerabilidad	Primera detección	Última actividad
Microsoft Office	Signed	Microsoft Corporation	5	Critical	2025-08-26 10:44:16	2025-08-29 08:19:04

Análisis de riesgos:

Aplicación: Microsoft Office

- Proveedor (vendor): Microsoft Corporation
- Firma digital: Signed
- Reputación: 5
- Vulnerabilidad detectada: Critical
- Actividad reciente: Vista por última vez el 2025-08-29 08:19:04
- Política aplicada: Default Communication Control Policy - Servers Policy - Isolation Policy
- Acción: According to policy – Manually - According to policy
- Observaciones: Se ha detectado una versión de Microsoft Office (16.0.10417.20042) con una vulnerabilidad clasificada como crítica, lo que representa un riesgo elevado para la seguridad del entorno. Aunque la aplicación proviene de un proveedor confiable y está firmada digitalmente, la reputación de esta versión específica es desconocida, lo cual incrementa la incertidumbre sobre su estabilidad y exposición.

Políticas de control aplicadas:

Política aplicada	Acción	Comentario
Default Communication Control Policy	According to policy	La acción fue permitida
Servers Policy	Manually	La acción fue permitida
Isolation Policy	According to policy	La acción fue denegada

Vulnerabilidades:

CVE-2025-53766: La vulnerabilidad permite a un atacante remoto ejecutar código arbitrario en el sistema de destino. La vulnerabilidad existe debido a un error de límite en GDI+. Un atacante remoto puede pasar datos especialmente diseñados a la aplicación, provocar un desbordamiento de búfer basado en el montón y ejecutar código arbitrario en el sistema objetivo. La explotación exitosa de esta vulnerabilidad puede resultar en el compromiso completo del sistema vulnerable.

CVE-2025-53732: La vulnerabilidad permite que un atacante remoto comprometa el sistema vulnerable. La vulnerabilidad existe debido a un error de uso tras la liberación en Microsoft Office. Un atacante remoto puede ejecutar código arbitrario en el sistema objetivo.

CVE-2025-30388: La vulnerabilidad permite a un atacante remoto ejecutar código arbitrario en el sistema de destino.
La vulnerabilidad existe debido a un error de límite en el componente gráfico de Windows. Un atacante remoto puede engañar a la víctima para que abra un archivo especialmente diseñado, provocar un desbordamiento de búfer basado en el montón y ejecutar código arbitrario en el sistema objetivo.
La explotación exitosa de esta vulnerabilidad puede resultar en el compromiso completo del sistema vulnerable.

CVE-2025-26687: La vulnerabilidad permite que un usuario local comprometa el sistema vulnerable.

La vulnerabilidad existe debido a un error de uso tras liberación en Win32k. Un usuario local puede superar una condición de carrera y obtener privilegios elevados en el sistema.

CVE-2025-21338: La vulnerabilidad permite a un atacante remoto ejecutar código arbitrario en el sistema de destino.
La vulnerabilidad existe debido a un desbordamiento de enteros en GDI+. Un usuario remoto puede pasar datos especialmente diseñados a la aplicación, provocar un desbordamiento de enteros y ejecutar código arbitrario en el sistema objetivo.
La explotación exitosa de esta vulnerabilidad puede resultar en el compromiso completo del sistema vulnerable.

CVE-2023-36565: La vulnerabilidad permite a un usuario local aumentar privilegios en el sistema.
La vulnerabilidad existe debido a una condición de carrera en Microsoft Office Graphics. Un usuario local puede explotar la condición de carrera y obtener acceso no autorizado a información confidencial y escalar privilegios en el sistema.

Productos y versiones afectados:

Producto: Microsoft Office
Versión: 16.0.10417.20042

Acciones de mitigación:

Instalar la actualización desde el sitio web del proveedor.

Recomendaciones:

- Validar las aplicaciones sin firma o de vendor desconocido.
- Realizar análisis de comportamiento (sandbox, análisis forense, etc.) a binarios desconocidos.
- Aplicar actualizaciones de seguridad a versiones vulnerables.
- Revisar y ajustar las políticas de comunicación para prevenir posibles brechas.
- Consultar con el equipo de desarrollo interno si alguna aplicación podría ser legítima pero no registrada.

Conclusiones:

Durante el periodo de análisis comprendido en este informe semanal, se identificaron aplicaciones con distintos niveles de riesgo que podrían comprometer la seguridad de la red si no se gestionan adecuadamente.

Las recomendaciones presentadas buscan fortalecer la postura de seguridad general, minimizando la exposición a amenazas internas o externas que puedan derivar en pérdida de integridad, confidencialidad o disponibilidad de los sistemas institucionales.