CSIRTSALUD-AL-20250911-29

TLP: AMBER

Alerta Id	0029
Fecha del reporte	11/09/2025
Entidad	Centro Dermatológico Federico Lleras Acosta
Título	Reporte semanal de monitoreo y gestión de aplicaciones en endpoints
Herramienta de detección	FortiEDR
Tipo de alerta	Vulnerabilidad
Nivel de riesgo	Critical

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 **04/09/2025 – 11/09/2025**. 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	Microsoft Corporation	Microsoft Corporation	Known good	Critical	2025-09-10 11:24:54	2025-09-11 07:49:43

Análisis de riesgos:

Aplicación: Microsoft® Office

- Proveedor (vendor): Microsoft Corporation
- Firma digital: Microsoft® Office
- Reputación: Known good
- Vulnerabilidad detectada: Critical
- Actividad reciente: 2025-09-10 11:24:54
- Política aplicada:Default Communication Control Policy
- Acción: Allow
- Política aplicada:Isolation Policy
- Acción: Deny
- Política aplicada:Servers Policy
- Acción: Allow

- Observaciones: Debido a la detección de vulnerabilidades High (alta) y Critical (Crítica), se identificó una posible contradicción en la confiabilidad del ejecutable Microsoft® Office. La acción tomada fue permitida, denegada y permitida se da comunicación para prevenir riesgos asociados a posibles compromisos de seguridad.

Políticas de control aplicadas:

Política aplicada	Acción	Comentario
Default Communication Control Policy	Allow	Comunicación permitida por política base; no se identificó actividad anómala.
Servers Policy	Allow	Comunicación permitida por política base; no se identificó actividad anómala.
Isolation Policy	Deny	Bloqueo activado por comportamiento sospechoso; posible riesgo de compromiso.

Actualizaciones:

Microsoft® Office v. 14. 0. 0370. 400 presenta varias vulnerabilidades, con severidades que varían de altas y medias, que comprometen la seguridad del sistema. los cuales se detallan a continuación:

CVE	Severidad	Descripción breve
CVE-2025-53766	CRITICAL	Permite que un atacante no autenticado ejecute código arbitrario de forma remota explotando documentos.
CVE-2025-30388	HIGH	Puede ser explotada localmente para escalar privilegios a nivel de sistema mediante un desbordamiento en el kernel.
CVE-2023-36565	HIGH	Posibilita la ejecución arbitraria de código a través de fallos en GDI+, impactando directamente la confidencialidad e integridad de la información.
CVE-2025-26687	HIGH	Abre la puerta a una elevación de privilegios mediante un fallo de memoria en Win32K, lo que facilita el control del sistema por un atacante autenticado.
CVE-2025-53732	HIGH	Afecta a Microsoft Office en dispositivos móviles y de escritorio, permitiendo ejecución de código malicioso si el usuario abre documentos manipulados, mientras que
CVE-2025-21338	HIGH	Habilita la escalada de privilegios en Office, incrementando el riesgo de abuso de cuentas con bajos permisos.

Productos y versiones afectados:

- Producto: Microsoft® Office
- Versión: 14. 0. 0370. 400
- Impacto: Afecta equipos y entornos donde Microsoft® Office versión 14. 0. 0370. 400 permite desde la ejecución remota de código sin autenticación hasta la escalada de privilegios locales, afectando tanto al sistema operativo como a Microsoft Office en distintas plataformas. En conjunto, exponen los equipos a compromiso total, pérdida de confidencialidad e integridad, y al riesgo de que atacantes obtengan control completo del sistema o abusen de cuentas con bajos permisos.

Acciones de mitigación:

Las acciones de mitigación recomendadas incluyen aplicar de inmediato los parches de seguridad oficiales de Microsoft, priorizando la CVE-2025-53766 por su criticidad, así como mantener actualizado Microsoft Office en la versión 14. 0. 0370. 400 . Es fundamental restringir los privilegios de usuario bajo el principio de mínimo privilegio, implementar segmentación de red y controles de acceso para reducir la exposición, y reforzar la seguridad en la apertura de archivos mediante soluciones EDR/antivirus actualizados. Además, se recomienda monitorear registros y alertas en busca de comportamientos anómalos relacionados con GDI+ y Win32K, y probar las actualizaciones en entornos controlados antes de su despliegue en producción para garantizar estabilidad en sistemas críticos.

Recomendaciones:

- Aplicar sin demora los parches de seguridad.
- Mantener actualizado Microsoft Office y Windows.
- Restringir privilegios de usuario y cuentas administrativas.
- Monitorear de forma continua los sistemas y registros de seguridad.

Conclusiones:

Durante el periodo de análisis comprendido en este informe semanal, se identificó una aplicación que podría comprometer la seguridad de la red si no se gestionan adecuadamente.

El sistema EDR ha aplicado correctamente las políticas de control establecidas, permitiendo bloquear o limitar el tráfico generado por componentes sospechosos. No obstante, se requiere un seguimiento puntual sobre ciertas aplicaciones sin procedencia clara, así como una revisión constante del estado de actualización de los programas críticos utilizados por la organización.

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.