

Alerta Id	0026
Fecha del reporte	2025/09/04
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	Alta

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 **28/08/2025 – 04/09/2025**. 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
McAfee WebAdvisor	McAfee	McAfee, LLC	Unknown	High	2025-09-02 14:17:04	2025-09-02 14:17:04
Adobe Download Manager	Adobe Systems	Adobe Inc	Contradiction	High	2025-08-30 10:51:01	2025-08-30 10:51:01

Ánalisis de riesgos:**Aplicación: McAfee WebAdvisor**

- Proveedor (vendor): McAfee, LLC
- Firma digital: McAfee
- Reputación: Unknown
- Vulnerabilidad detectada: High
- Actividad reciente: 2025-09-02 14:17:04
- Política aplicada: Servers Policy, Isolation Policy
- Acción: Deny
- Observaciones: Debido a la detección de vulnerabilidades High (alta), se identificó una posible contradicción en la confiabilidad del ejecutable McAfee WebAdvisor. La acción tomada fue Deny, bloqueando su ejecución y comunicación para prevenir riesgos asociados a posibles compromisos de seguridad.

Aplicación: Adobe Download Manager

- Proveedor (vendor): Adobe Inc
- Firma digital: Adobe Systems
- Reputación: Contradiction
- Vulnerabilidad detectada: High
- Actividad reciente: 2025-08-30 10:51:01
- Política aplicada: Servers Policy, Isolation Policy
- Acción: Deny
- Observaciones: Debido a la detección de vulnerabilidades High (alta) y contradicciones en la reputación del ejecutable. La acción tomada fue Deny, bloqueando la ejecución o

comunicación del software potencialmente comprometido.

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	Deny	Acceso denegado por política de servidores; el ejecutable intentó conectar con IPs no autorizadas.
Isolation Policy	Deny	Bloqueo activado por comportamiento sospechoso; posible riesgo de compromiso.

Actualizaciones:

McAfee WebAdvisor v. 4.1.1.1064 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-2022-0815	Alta	Escalamiento de privilegios locales debido a validación incorrecta en McAfee WebAdvisor.
CVE-2019-3670	Media	XSS en McAfee ePolicy Orchestrator; permite inyección de scripts vía parámetros web.

En cuanto a Adobe Download Manager v. 2.0.0.820s también presenta varias vulnerabilidades, con severidades que varían de altas y medias, de las cuales se detallan a continuación:

CVE	Severidad	Descripción breve
CVE-2010-0189	Alta	Ejecución remota de código en Microsoft Internet Explorer a través de una vulnerabilidad en el componente ActiveX (msvidctl.dll).
CVE-2022-2926	Media	Vulnerabilidad en Google Chrome que permite eludir políticas de seguridad mediante manipulación de extensiones.
CVE-2006-5856	Media	Desbordamiento de búfer en Adobe Download Manager que puede permitir ejecución arbitraria de código al procesar entradas manipuladas.

Productos y versiones afectados:

- Producto: McAfee WebAdvisor
- Versión: 4.1.1.1064
- Impacto: Afecta equipos y entornos donde McAfee WebAdvisor versión 4.1.1.1064 esté instalado sin actualizaciones de seguridad, lo que puede permitir escalamiento de privilegios, ejecución de código no autorizado o establecimiento de comunicaciones no confiables con servidores externos.
- Producto: Adobe Download Manager
- Versión: 2.0.0.820s
- Impacto: Afecta equipos y entornos especialmente si se encuentra desactualizado o con reputación desconocida. Esta versión puede exponer el sistema a riesgos de ejecución de código arbitrario o explotación de vulnerabilidades antiguas, facilitando posibles vectores de ataque como desbordamientos de búfer o manipulación de entradas no seguras.

Acciones de mitigación:

Se recomienda actualizar inmediatamente McAfee WebAdvisor a la versión más reciente disponible que contenga parches para vulnerabilidades críticas como el posible escalamiento de privilegios. De igual forma, se debe reemplazar o eliminar versiones desactualizadas de Adobe Download Manager, como la 2.0.0.820s, debido a los riesgos asociados a la ejecución de código. Es fundamental reforzar las políticas de seguridad en el entorno, aplicando controles como Application Control, Isolation Policy y restricciones de ejecución por reputación, a fin de limitar el impacto de posibles compromisos. Se recomienda mantener prácticas de actualización periódica, capacitación técnica al personal responsable de la gestión de software y seguridad.

Recomendaciones:

- 
- Validar las aplicaciones sin firma o de vendedor desconocido.
 - 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 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.