Incidente Id	0010
Fecha del reporte	2025/08/08
Entidad	Centro Dermatológico Federico Lleras Acosta
Título	Reporte semanal de monitoreo y gestión de aplicaciones en endpoints
Herramienta de detección	FortiEDR
Tipo de incidente	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 **31/07/2025 – 07/08/2025**. 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
FortiClient	Fortinet	FortiClient	Contradiction	Critical	2025-07-31 16:23:43	2025-07-31 16:23:43

Análisis de riesgos:

Aplicación: Forticlient

- Proveedor (vendor): FortiClient
- Firma digital: Fortinet
- Reputación: Contradiction
- Vulnerabilidad detectada: Critical
- Actividad reciente: 2025-07-31 16:23:43.
- Política aplicada: Servers Policy, Isolation Policy
- Acción: Deny
- Observaciones: Debido a la detección de vulnerabilidades críticas 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:

FortiClient v. 7.0.9.493 presenta varias vulnerabilidades, con severidades que varían de críticas a bajas, que comprometen la seguridad del sistema. los cuales se detallan a continuación:

CVE	Severidad	Descripción breve
CVE-2023-45590	Crítico	Ejecución remota o escalamiento de privilegios
CVE-2024-47574	Alta	Bypass de autenticación local en FortiClient Windows usando tuberías nombradas; permite ejecución privilegiada.
CVE-2024-36513	Alta	Escalamiento de privilegios por error en scripts de actualización automática (Windows).
CVE-2024-31489	Alta	Validación incorrecta de certificados permite ataques MitM en túneles ZTNA.
CVE-2024-36507	Alta	Ruta de búsqueda no confiable permite ejecución de DLLs maliciosas (DLL hijacking).
CVE-2024-3661	Alta	Tráfico VPN puede filtrarse a través de interfaces físicas por fallo en DHCP.
CVE-2024-50570	Media	Contraseñas VPN almacenadas en texto claro en memoria; accesibles por usuarios autenticados.
CVE-2024-54019	Media	Falla en autenticación o tráfico VPN
CVE-2024-40586	Media	Escalamiento de privilegios locales vía acceso indebido al servicio FortiSSLVPNd.
CVE-2022-45856	Media	Permite a los atacantes causar una denegación de servicio (DoS)

CVE-2024-50564	Baja	Uso de clave criptográfica embebida permite descifrado de comunicaciones entre procesos.

Productos y versiones afectados:

- Producto: FortiClient
- Versión: 7.0.9.493
- Impacto: Afecta equipos y entornos donde FortiClient esté instalado sin parches de seguridad, lo que puede permitir escalamiento de privilegios, filtración de datos o ejecución de código no autorizado.

Acciones de mitigación:

Se recomienda actualizar inmediatamente FortiClient a la versión más reciente que incluya correcciones para las vulnerabilidades críticas y altas identificadas. Además, es fundamental reforzar la configuración del entorno aplicando políticas de seguridad como Servers Policy e Isolation Policy, a fin de restringir la ejecución no autorizada y limitar el alcance de posibles ataques. Es clave mantener al personal técnico capacitado en buenas prácticas de ciberseguridad y asegurar un ciclo de actualización regular del software y sus componentes asociados.

Recomendaciones:

- Validar las aplicaciones sin firma o de vendor 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.