Incidente Id	0015
Fecha del reporte	2025/08/14
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	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 **07/08/2025 – 14/08/2025**. Se identificó una aplicación activa con riesgo alto.

Aplicaciones destacadas:

Aplicación	Firma	Vendor	Reputación	Vulnerabilidad	Primera detección	Última actividad
Google Update	Google	Google	Contradiction	High	2025-08-12 19:50:23	2025-08-12 19:50:47

Análisis de riesgos:

Aplicación: Google Update

- Proveedor (vendor): Google Update
- Firma digital: Google
- Reputación: Contradiction
- Vulnerabilidad detectada: High
- Actividad reciente: 2025-08-12 19:50:47
- Política aplicada: Servers Policy, Isolation Policy
- Acción: Deny
- Observaciones: Debido a la detección de vulnerabilidad alta, la intención de actualización de Google fue denegada.

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:

Google Update v. 1. 3. 36. 121 presenta varias vulnerabilidades, con severidad alta, que comprometen la seguridad del sistema. los cuales se detallan a continuación:

CVE	Severidad	Descripción breve
CVE-2024-1694	High	Es una implementación incorrecta de google Update anterior a la versión 1. 3. 36. 121, eludiendo el control de acceso
CVE-2023-7261	High	Un atacante no autenticado ejecute comando del sistema operativo

Productos y versiones afectados:

- Producto: Google Update
- Versión: 1. 3. 36. 121
- Impacto: Afecta equipos y entornos donde Google Update esté instalado sin parches de seguridad, lo cual puede ejecutar comandos, códigos y accesos no autorizados.

Acciones de mitigación:

Realizar la desinstalación del navegador Google, descargar desde la página oficial la última versión de este navegador. Verificar que el antivirus se encuentre en la última versión, una vez identificado realizar un escaneo para descartar posibles infecciones.

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.