Incidente Id	0009
Fecha del reporte	2025/07/31
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 **24/07/2025 – 31/07/2025**. 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
Node.js	Node.js Foundation	Node.js	Contradiction	Critical	31/07/2025 8:53:34 a. m.	31/07/2025 8:53:39 a. m.

Análisis de riesgos:

Aplicación: Node.js

- Proveedor (vendor): Node.js
- Firma digital: Node.js Foundation
- Reputación: Contradiction
- Vulnerabilidad detectada: Critical
- Actividad reciente: 31/07/2025 8:53:39 a. m.
- Política aplicada: Servers Policy, Isolation Policy
- Acción: Deny
- Observaciones: Debido a la detección de vulnerabilidades críticas y contradicciones en la reputación del ejecutable, se ha denegado el acceso conforme a las políticas de Servidores de aislamiento para prevenir riesgos de seguridad.

Políticas de control aplicadas:

Política aplicada	Acción	Comentario
Default Communication Control Policy	Allow	Comunicación permitida según la política base, aunque el ejecutable no está firmado
Servers Policy	Deny	Bloqueado por política de servidores: la aplicación intentó comunicarse con múltiples IPs no autorizadas.
Isolation Policy	Deny	La aplicación fue denegada por comportamiento sospechoso; ejecutable sin firma válida.

Actualizaciones:

Node.js versión 12.14.0 presenta múltiples vulnerabilidades con niveles de gravedad que van de críticos a medios, los cuales se detallan a continuación:

CVE	Severidad	Descripción breve
CVE-2024-3566	Crítico	Ejecución remota de código por manejo incorrecto de entradas.
CVE-2021-22931	Crítico	Escalamiento de privilegios local en módulos específicos.
CVE-2021-22930	Crítico	Vulnerabilidad en manejo de memoria que puede causar corrupción.
CVE-2019-15606	Crítico	Desbordamiento de búfer con riesgo de ejecución remota.
CVE-2019-15605	Crítico	Desbordamiento de búfer similar al CVE-2019-15606.
CVE-2022-21824	Alto	Vulnerabilidad de seguridad alta con posible impacto en integridad.

CVE	Severidad	Descripción breve
CVE-2022-0778	Alto	Riesgo alto por vulnerabilidad en componentes de red.
CVE-2021-44531	Alto	Posible vulnerabilidad en validación de entradas.
CVE-2021-3450	Alto	Vulnerabilidad relacionada con certificados y validaciones SSL.
CVE-2021-23840	Alto	Riesgo alto en manejo de procesos internos.
CVE-2021-22940	Alto	Vulnerabilidad alta en componentes de autenticación.
CVE-2021-22921	Alto	Riesgo de seguridad alto en dependencias internas.
CVE-2021-22884	Alto	Posible escalamiento de privilegios.
CVE-2021-22883	Alto	Vulnerabilidad en manejo de memoria.
CVE-2020-8265	Alto	Riesgo de seguridad alto con impacto en la estabilidad.
CVE-2020-8252	Alto	Riesgo alto en procesamiento de datos.
CVE-2020-8201	Alto	Riesgo alto en validación de datos.
CVE-2020-8174	Alto	Vulnerabilidad alta en módulos de red.
CVE-2020-8172	Alto	Riesgo alto en gestión de memoria.
CVE-2020-11080	Alto	Riesgo alto en ejecución de procesos.
CVE-2019-15604	Alto	Riesgo alto en manejo de memoria similar a CVE-2019-15606.
CVE-2021-44533	Medio	Vulnerabilidad de severidad media en validación.
CVE-2021-44532	Medio	Riesgo medio en el manejo de configuraciones.
CVE-2021-3672	Medio	Riesgo medio en integridad de datos.
CVE-2021-3449	Medio	Vulnerabilidad media en manejo de certificados.
CVE-2021-22939	Medio	Vulnerabilidad media en autenticación.
CVE-2021-22918	Medio	Riesgo medio en el procesamiento interno.
CVE-2020-8287	Medio	Vulnerabilidad media en manejo de memoria.
CVE-2020-1971	Medio	Riesgo medio en validación y seguridad general.

Productos y versiones afectados:

- Producto: Node.js
- Versión: 12.14.0
- Impacto: Afecta servidores y aplicaciones que usen esta versión sin parches o actualizaciones de seguridad.

Acciones de mitigación:

Se recomienda actualizar inmediatamente Node.js a la versión más reciente que incluya parches para las vulnerabilidades críticas y altas identificadas. Además, es fundamental aplicar todas las políticas de seguridad disponibles, como la Servers Policy y Isolation Policy, para limitar la ejecución y el acceso de la aplicación afectada. Es importante implementar controles adicionales como el monitoreo constante de la actividad del sistema para detectar comportamientos anómalos, y utilizar técnicas de aislamiento, como contenedores o sandboxing, para minimizar el impacto en caso de explotación. Finalmente, se debe fomentar la capacitación continua del personal técnico para mantener buenas prácticas de seguridad y asegurar la actualización constante del software y sus dependencias.

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.