Incidente Id	0020
Fecha del reporte	2025/08/29
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 **21/08/2025 – 28/08/2025**. Se identificó una aplicación activa con riesgo alto.

Aplicaciones destacadas:

Aplicación	Firma	Vendor	Reputación	Vulnerabilidad	Primera detección	Última actividad
Autodesk Design Review	Autodesk	Autodesk	Unknown	High	2025-08-21 08:34:58	2025-08-21 08:34:59

Análisis de riesgos:

Aplicación: Autodesk Design Review

- Proveedor (vendor): Autodesk
- Firma digital: Signed
- Reputación: Unknown
- Vulnerabilidad detectada: High
- Actividad reciente: 2025-08-21 08:34:59
- Política aplicada: Default Communication Control
- Acción: Deny
- Observaciones: Debido a la detección de vulnerabilidad alta, la intención de ejecución de Autodesk Design Review 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:

Autodesk Design Review update v. 15. 0. 2. 10 presenta varias vulnerabilidades, con severidad alta, que comprometen la seguridad del sistema. los cuales se detallan a continuación:

CVE	Severidad	Descripción breve
CVE-2022-33889	High	Es un desbordamiento de búfer en memoria que puede explotarse al abrir archivos GIF o JPEG manipulados. Esto permite a un atacante ejecutar código arbitrario con los privilegios del usuario que ejecute la aplicación, lo que representa un riesgo alto de compromiso del sistema si no se aplican las actualizaciones de seguridad correspondientes.

Productos y versiones afectados:

- Producto: Autodesk Design Review
- Versión: 15. 0. 2. 10
- Impacto: Afecta equipos y entornos donde Autodesk Design Review 15.0.2.10 esté instalado sin parches de seguridad, lo cual puede permitir la ejecución de código arbitrario al abrir archivos maliciosos, provocando accesos no autorizados, robo de información o compromiso total del sistema.

Acciones de mitigación:

Realizar la desinstalación de Autodesk Design Review 15.0.2.10, descargar desde la página oficial de Autodesk la última versión corregida o el Hotfix correspondiente. Verificar que el antivirus o EDR se encuentre actualizado a su última versión y, posteriormente, ejecutar un escaneo completo para descartar posibles infecciones derivadas de la vulnerabilidad.

Recomendaciones:

- Validar que la instalación de Autodesk Design Review 15.0.2.10 provenga de una fuente oficial y no de un proveedor desconocido.
- Aplicar las actualizaciones de seguridad o el Hotfix liberado por Autodesk para corregir la vulnerabilidad CVE-2022-33889.
- Revisar y ajustar las políticas de manejo de archivos externos (GIF/JPEG) para prevenir la apertura de contenido malicioso.
- Consultar con el equipo de desarrollo o de arquitectura si alguna aplicación interna depende de esta versión y planificar su actualización o reemplazo seguro.

Conclusiones:

Durante el periodo de análisis comprendido en este informe semanal, se identificó que la versión 15.0.2.10 de Autodesk Design Review presenta la vulnerabilidad CVE-2022-33889, la cual podría comprometer la seguridad de los equipos al permitir la ejecución de código arbitrario si no se gestiona adecuadamente.

El sistema EDR ha aplicado correctamente las políticas de control establecidas, permitiendo bloquear ciertas acciones sospechosas generadas por la aplicación. No obstante, se requiere un seguimiento puntual sobre esta versión vulnerable y una verificación constante del estado de actualización de los programas críticos utilizados en la organización.

Las recomendaciones presentadas buscan fortalecer la postura de seguridad general, reduciendo la exposición frente a intentos de explotación que puedan derivar en pérdida de integridad, confidencialidad o disponibilidad de los sistemas institucionales.