Alerta Id	0021
Fecha del reporte	2025/08/29
Entidad	Fondo de Previsión Social del Congreso de la República
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 **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
HP Support Assistant	Hewlett-Packard	Hewlett-Packard	Contradiction	High	2025-08-25 14:31:36	2025-08-25 14:31:39

Análisis de riesgos:

Aplicación: HP Support Assistant

- Proveedor (vendor): Hewlett-Packard
- Firma digital: Hewlett-Packard
- Reputación: Contradiction
- Vulnerabilidad detectada: High
- Actividad reciente: 2025-08-25 14:31:39
- Política aplicada:
  - Default Communication Control Policy - Acción: Allow
  - Servers Policy - Acción: Deny
  - Isolation Policy - Acción: Allow
- Observaciones: Debido a la detección de múltiples vulnerabilidades críticas y altas, la ejecución del servicio HP Support Assistant 7.7.40.2 fue restringida parcialmente por las políticas de control establecidas.

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	Allow	Bloqueo activado por comportamiento sospechoso; posible riesgo de compromiso.

Actualizaciones:

Autodesk Design Review update v. 7. 7. 40. 2 presenta varias vulnerabilidades, con severidad alta, que comprometen la seguridad del sistema. los cuales se detallan a continuación:

CVE	Severidad	Descripción breve
CVE-2020-6919	High	Es una vulnerabilidad que permite a un atacante ejecutar código arbitrario mediante archivos manipulados, comprometiendo la integridad y confidencialidad del sistema.
CVE-2019-6329	High	Permite la ejecución de código no autorizado al explotar fallos de validación en el software, lo que puede derivar en accesos indebidos al sistema.
CVE-2020-6917	High	Es una falla que posibilita la elevación de privilegios al procesar datos maliciosos, permitiendo que un atacante tome control del equipo afectado.
CVE-2022-23453	High	Corresponde a un error de seguridad que puede explotarse para obtener ejecución de código en el dispositivo, representando un riesgo de compromiso crítico si no se aplica el parche.
CVE-2022-23455	High	Una vulnerabilidad que facilita la ejecución remota de código al aprovechar un fallo en el manejo de entradas, lo que expone al sistema a accesos no autorizados.

CVE	Severidad	Descripción breve
CVE-2022-23454	High	Es una debilidad en la validación de datos que permite a atacantes inyectar código malicioso, comprometiendo la seguridad y estabilidad del sistema afectado.
CVE-2020-6921	High	Vulnerabilidad que habilita la ejecución arbitraria de comandos al abrir archivos manipulados, permitiendo control indebido sobre el entorno del usuario.
CVE-2019-6328	High	Permite a un atacante remoto ejecutar código arbitrario mediante la explotación de un fallo en la aplicación, lo que representa un alto riesgo de intrusión.
CVE-2018-5927	High	Se trata de un error que facilita la escalada de privilegios y acceso indebido a recursos críticos, aumentando la exposición a ataques dirigidos.
CVE-2020-6918	High	Vulnerabilidad que puede ser explotada para ejecutar código en el contexto del usuario, con impacto en la confidencialidad y disponibilidad del sistema.
CVE-2020-6922	High	Permite la manipulación de procesos internos para lograr ejecución no autorizada de código, afectando la seguridad de la red y los equipos vinculados.
CVE-2022-38395	High	Falla de seguridad que posibilita a un atacante remoto ejecutar código arbitrario, comprometiendo la integridad del sistema si no se actualiza.

Productos y versiones afectados:

- Producto: HP Support Assistant
- Versión: 7. 7. 40. 2
- Impacto: Las múltiples vulnerabilidades críticas y de alta severidad presentes en HP Support Assistant 7.7.40.2 permiten a un atacante ejecutar código arbitrario, escalar privilegios, manipular procesos internos y obtener accesos no autorizados mediante la explotación de archivos o datos manipulados. Esto afecta tanto a equipos individuales como a entornos corporativos donde la aplicación esté instalada sin parches de seguridad, exponiendo la red a riesgos de intrusión, robo de información sensible, pérdida de integridad y disponibilidad de los sistemas. El impacto potencial incluye el compromiso total de los equipos afectados, su uso como punto de entrada para movimientos laterales en la red y la posibilidad de ataques dirigidos que deriven en interrupción de operaciones críticas.

Acciones de mitigación:

Realizar la desinstalación de HP Support Assistant 7.7.40.2 y descargar desde la página oficial de HP 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 las vulnerabilidades detectadas.

Recomendaciones:

- Validar que la instalación de HP Support Assistant provenga siempre de la página oficial de HP y no de fuentes desconocidas.
- Aplicar las actualizaciones de seguridad liberadas por HP para mitigar las vulnerabilidades críticas identificadas.
- Revisar y ajustar las políticas de seguridad en la organización para restringir la ejecución de aplicaciones obsoletas y prevenir accesos indebidos.
- Consultar con el equipo de TI si alguna herramienta o proceso interno 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 7.7.40.2 de HP Support Assistant presenta múltiples vulnerabilidades críticas y de alta severidad, que podrían comprometer la seguridad de los equipos al permitir la ejecución de código arbitrario, la elevación de privilegios y accesos no autorizados si no se gestionan adecuadamente.

El sistema de seguridad aplicó correctamente políticas de control, restringiendo parcialmente las acciones sospechosas de la aplicación. Sin embargo, se requiere un seguimiento puntual sobre esta versión vulnerable y una verificación constante del estado de actualización de los programas críticos utilizados por 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.