Alerta Vulnerabilidad
Vulnerabilidad Crítica en Adobe Reader y DC

CSIRTSALUD-AV-20260413-41 **TLP: CLEAR**

Alerta ID:	041
Fecha del reporte:	13/04/2026
Entidad:	Todas las Entidades del Ecosistema Digital
Título:	Vulnerabilidad Crítica en Adobe Acrobat Reader y DC
Herramienta de detección	N/A
Activo involucrado:	Adobe Acrobat Reader
Tipo de alerta:	Boletín informativo
Nivel de riesgo:	Alta

Resumen ejecutivo

Informar a las entidades del Ecosistema salud sobre la vulnerabilidad crítica identificada como CVE-2026-34621, detectada en Adobe Acrobat Reader y Adobe Acrobat DC. Esta vulnerabilidad, catalogada como zero-day, ha sido confirmada por Adobe como explotada activamente en la naturaleza desde, al menos, diciembre de 2025.

CSIRT Salud emite este boletín con el fin de orientar a los equipos técnicos y de gestión de seguridad de la información de las entidades del sector para la adopción oportuna de medidas de detección, contención y remediación, dado el riesgo que representa para la integridad, confidencialidad y disponibilidad de los sistemas de información y datos clínicos.

Descripción:

CVE-2026-34621 es una vulnerabilidad de tipo Prototype Pollution (contaminación de prototipo) presente en el motor JavaScript integrado de Adobe Acrobat Reader. Fue

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

descubierta por el investigador de seguridad Haifei Li, fundador de EXPMON, sistema público de detección de exploits avanzados, luego de que un usuario enviará para análisis un archivo PDF malicioso denominado yummy_adobe_exploit_uwu.pdf el 26 de marzo de 2026.

El análisis forense posterior reveló que la muestra había sido subida a VirusTotal tres días antes, con una tasa de detección inicial de apenas 5/64, lo que evidencia el alto nivel de evasión antiforense del exploit. Investigaciones adicionales indicaron que la explotación habría comenzado en diciembre de 2025, manteniéndose sin detección pública durante más de cuatro meses.

El ataque sigue una cadena bien definida que combina ingeniería social, explotación de la vulnerabilidad y reconocimiento del sistema víctima:

- Distribución mediante phishing: Los actores de amenaza distribuyen documentos PDF maliciosos a través de correos electrónicos de phishing, disfrazados como facturas, informes clínicos, comunicaciones oficiales o solicitudes de expedientes médicos, aprovechando la alta confianza que los usuarios depositan en el formato PDF.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

- Apertura del archivo cebo: Basta con que la víctima abra el archivo PDF en una versión vulnerable de Adobe Acrobat Reader para desencadenar el exploit; no se requiere ninguna interacción adicional más allá del acto de apertura.
- Inyección de JavaScript malicioso: El PDF contiene JavaScript especialmente diseñado que aprovecha la falla de Prototype Pollution para manipular los objetos internos del motor JavaScript de Acrobat.
- Abuso de APIs privilegiadas: El exploit invoca APIs privilegiadas como util.readFileIntoStream() para leer archivos arbitrarios del sistema y RSS.addFeed() para exfiltrar datos y obtener código controlado por el atacante.
- Reconocimiento (fingerprinting) del sistema: El exploit ejecuta un perfil detallado del sistema víctima, recopilando información del entorno antes de decidir si ejecutar la segunda etapa del ataque.
- Comunicación con servidor C2: Los datos recolectados son enviados a un servidor de Comando y Control (C2) operado por los atacantes, incluyendo tráfico con el identificador de User Agent 'Adobe Synchronizer'.

Consecuencias de la Explotación

La explotación exitosa de CVE-2026-34621 puede resultar en las siguientes consecuencias de alto impacto:

IMPACTO	DESCRIPCIÓN
Ejecución de código arbitrario	El atacante puede ejecutar código malicioso con los privilegios del usuario que abrió el PDF, lo que le permite instalar malware, ransomware o herramientas de acceso remoto (RAT) en el sistema comprometido.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

IMPACTO	DESCRIPCIÓN
Exfiltración de archivos locales	A través de la API util.readFileIntoStream(), el atacante puede acceder y extraer archivos a los que el proceso de Adobe Reader tiene acceso en el sandbox, incluyendo credenciales, historias clínicas u otros documentos sensibles.
Reconocimiento y huella digital del sistema	El exploit puede recopilar información detallada del sistema (OS, versión de software, rutas de archivos, configuración de red) y enviarla al servidor C2, facilitando la planeación de ataques dirigidos adicionales.
Movimiento lateral	Una vez establecido en el sistema, el atacante puede intentar desplazarse lateralmente hacia otros sistemas en la red institucional, escalando privilegios y comprometiendo infraestructura crítica.
Compromiso de confidencialidad	La sustracción de datos clínicos, credenciales o información personal identificable (PII) de pacientes pone en riesgo el cumplimiento normativo bajo la Ley 1581 de 2012 (Protección de Datos) y resoluciones del Ministerio de Salud.
Interrupción de servicios	La instalación de ransomware u otro malware destructivo puede paralizar sistemas de información hospitalaria (HIS), sistemas PACS de imágenes diagnósticas o plataformas de telemedicina.
Persistencia a largo plazo	El acceso inicial puede permitir al atacante establecer mecanismos de persistencia (puertas traseras, tareas programadas, servicios maliciosos) que sobrevivan reinicios y actualizaciones del sistema.

Modo de explotación detallado.

Fase 1 — Preparación y armado del exploit

El actor de amenaza construye un archivo PDF especialmente diseñado que contiene código JavaScript ofuscado. Este código explota la falla CWE-1321 de Prototype Pollution: en

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

JavaScript, todos los objetos heredan propiedades de Object.prototype. Si la aplicación no valida correctamente las entradas, un atacante puede inyectar propiedades maliciosas en este prototipo compartido.

En el contexto de Adobe Acrobat Reader, el motor JavaScript integrado (Adobe's JavaScript engine basado en SpiderMonkey/V8) no filtra correctamente la modificación de atributos del prototipo base, permitiendo que el payload contamine el entorno de ejecución global de la aplicación.

Fase 2 — Distribución y entrega (Initial Access)

El PDF malicioso se distribuye mediante alguno de los siguientes vectores:

- Correos electrónicos de phishing dirigido (spear-phishing) con archivos adjuntos disfrazados como facturas, resultados de laboratorio, citaciones u órdenes de compra médica.
- Descargas desde sitios web comprometidos que sirven el PDF bajo pretexto de consultar documentos clínicos o administrativos del sector salud.
- Compartición a través de plataformas de mensajería institucional o repositorios documentales internos previamente comprometidos.

Fase 3 — Ejecución del exploit (Execution)

Al abrir el PDF, el motor JavaScript de Adobe Reader carga y ejecuta automáticamente el código contenido en el objeto /JavaScript del documento. El script inicia la cadena de explotación de Prototype Pollution: añade o modifica propiedades en Object.prototype que son heredadas por otros objetos internos del runtime de Acrobat, alterando el flujo de ejecución de funciones críticas de la aplicación.

Específicamente, el exploit aprovecha que ciertas APIs privilegiadas de Acrobat (normalmente restringidas al contexto privilegiado) se vuelven accesibles una vez que los controles de verificación del prototipo han sido adulterados, permitiendo invocar funciones como util.readFileIntoStream() y RSS.addFeed() sin restricciones del sandbox.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Fase 4 — Reconocimiento del sistema (Discovery)

Antes de ejecutar payloads adicionales, el exploit realiza una fase de fingerprinting del sistema víctima: recopila información sobre el sistema operativo, versión de Acrobat, rutas del sistema de archivos, configuración regional, presencia de soluciones de seguridad y privilegios del usuario actual. Esta información es enviada al servidor C2 a través de llamadas RSS.addFeed() o conexiones HTTP/HTTPS con el User-Agent 'Adobe Synchronizer', permitiendo a los atacantes seleccionar víctimas de alto valor.

Fase 5 — Exfiltración de archivos y ejecución de código (Collection / Command & Control)

Una vez confirmado el perfil de la víctima como objetivo de interés, el exploit usa util.readFileIntoStream() para leer archivos locales a los que el proceso de Reader tiene acceso dentro de su sandbox (documentos recientes, credenciales almacenadas, archivos de configuración). Los datos son exfiltrados al servidor C2. Paralelamente, RSS.addFeed() descarga y ejecuta código adicional del atacante, que puede incluir: droppers de malware, implantes de acceso remoto (RAT), ransomware u otras herramientas post-explotación.

Fase 6 — Post-explotación y persistencia

Una vez comprometido el sistema, los atacantes pueden establecer persistencia mediante:

- Creación de tareas programadas o servicios del sistema para mantener acceso tras reinicios.
- Instalación de implantes de acceso remoto para mantener canal C2 persistente.
- Escalada de privilegios hacia cuentas de administrador local o de dominio.
- Movimiento lateral hacia otros sistemas en la red institucional mediante credenciales robadas o vulnerabilidades de red.

Indicadores de compromiso

Los siguientes indicadores han sido identificados por investigadores de EXPMON, la comunidad de seguridad y los reportes de Adobe durante el análisis de las muestras maliciosas asociadas a CVE-2026-34621:

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

- **IOCs de Archivos y Red**

TIPO	VALOR / INDICADOR	DESCRIPCIÓN
Nombre de archivo	yummy_adobe_exploit_uwu.pdf	Primera muestra identificada enviada a EXPMON (26 mar 2026)
User-Agent HTTP	Adobe Synchronizer	Cadena de User Agent usada por el exploit para comunicación C2 — bloquear en proxy/firewall
Proceso sospechoso	AcroCEF.exe / acrobat.exe lanzando cmd.exe o powershell.exe	Indicativo de ejecución de código secundario desde Adobe Reader
API PDF abusada	util.readFileIntoStream()	Lectura de archivos arbitrarios del sistema local desde el contexto de Reader
API PDF abusada	RSS.addFeed()	Exfiltración de datos y descarga de payloads adicionales desde servidor C2
Extensión de archivo	*.pdf con JavaScript integrado	Archivos PDF con JS ofuscado en objetos /JavaScript o /JS del árbol de objetos
Detección AV inicial	5/64 en VirusTotal (23 mar 2026)	Alta evasión de motores antivirus en el momento de distribución inicial
Hash SHA256 (referencia)	Pendiente publicación Adobe/EXPMON	Consultar actualización en NVD y EXPMON para hash confirmado de muestras

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

- **Muestras PDF maliciosas confirmadas**

TIPO HASH	VALOR	TAMAÑO	DESCRIPCIÓN	VEREDICTO
SHA-256 (v2)	54077a5b15638e354fa02318623775b7a1cc0e8c21e59bcbab333035369e377f	320.066 B	Muestra principal (PDF 1.7) — Invoice540.pdf / yummy_adobe_exploit_uwu.pdf — C2: 188.214.34.20:34123 — Campaign ID: 422974	**MALICIOSO**
SHA-1 (v2)	dafd571da1df72fb53bcd250e8b901103b51d6e4	—	Hash SHA-1 correspondiente a la muestra v2 principal	**MALICIOSO**
MD5 (v2)	522cda0c18b410daa033dc66c48eb75a	—	Hash MD5 correspondiente a la muestra v2 principal	**MALICIOSO**
SSDEEP (v2)	6144:JeSqETXrhj1xWuSpMRdZKoEWmyduMPWG73E/eN2zpf6O:JeSqA5WGZKv3eOiO	—	Hash difuso — útil para detección de variantes similares	**REFERENCIA**
SHA-256 (v1)	65dca34b04416f9a113f09718cbe51e11fd58e7287b7863e37f393ed4d25dde7	254.698 B	Muestra prototipo (PDF 1.5) — primer envío a EXPMON — C2: 169.40.2.68:45191 — Campaign ID: 319988	**MALICIOSO**

- **Archivos descartados en el sistema víctima (Dropped Files)**

TIPO HASH	VALOR	TAMAÑO	DESCRIPCIÓN	VEREDICTO
SHA-256	eacad3e01b8b0a44ac030c8c169664dbbdde90c153b550c7b4e0609573df796d	5.932 B	Tmp97B7.tmp — Firma DER PKCS#7 de Adobe (timestamp legítimo)	**BENIGNO**
SHA-256	69bf0bc46f51b33377c4f3d92caf876714f6bbbe99e754448732792087 3f9820	4 B	ks_folder_watcher.txt — Texto ASCII (telemetría Adobe)	**BENIGNO**

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

TIPO HASH	VALOR	TAMAÑO	DESCRIPCIÓN	VEREDICTO
SHA-256	a2c2339691fc48fbd14fb307292dff3e21222712d9240810742d7df0c6d74dfb	2 B	s11[1] — Caché IE: respuesta del servidor C2 — Contenido: '//' (JS vacío). Confirma filtrado C2 en sandboxes.	**SOSPECHOSO**

- **Direcciones IP del servidor C2**

ROL	DIRECCIÓN IP	PUERTO	PAÍS / ASN	DETALLES DE INFRAESTRUCTURA
C2 PRIMARIO	188.214.34.20	**34123**	Chipre / AS57169	EDIS GmbH — Ubuntu Linux — OpenSSH 9.6p1 — Puerto 34123 NUNCA visible en Shodan (filtrado por IP). Hostname: 20.34.214.188.static.edisglobal.com. Registrado sep 2024. Asignado a rango 188.214.34.0/24.
C2 SECUNDARIO	169.40.2.68	**45191**	Letonia / AS42532	SIA VEESP — Sin datos Shodan, sin DNS pasivo, sin historial VT. IP completamente oscura — posiblemente dado de baja tras exposición por EXPMON. Detección VT: 1/94.

- **Dominios e infraestructura DNS**

DOMINIO / SUBDOMINIO	IP RESUELTA	REGISTRADO	DETALLES
ado-read-parser.com	—	2025-02-06	Registrar: NameSilo | Privacidad: privacyguardian.org | NS: dnsowl.com | VT: 0/94 detecciones | Sin cert. SSL (crt.sh) | Sin capturas Wayback | Expira: 2026-02-06
zx.ado-read-parser.com	188.214.34.20	DNS: 2025-07-08	Subdominio que apunta al C2 primario. Primera resolución DNS detectada el 8 jul 2025. Actualmente sin respuesta (dado de baja tras exposición).

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

- **Claves de registro (Persistencia)**

TIPO	CLAVE / VALOR DE REGISTRO	DESCRIPCIÓN
Run Key (persistencia)	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Adobe Reader Synchronizer	Mecanismo de persistencia principal. El exploit registra AdobeCollabSync.exe como proceso de inicio automático disfrazado de componente legítimo de Adobe.
Valor ejecutable	C:\Program Files\Adobe\Acrobat DC\Acrobat\AdobeCollabSync.exe	Ruta del ejecutable utilizado para la persistencia — proceso legítimo de Adobe abusado para evasión.
Servicios consultados	wscsvc, PcaSvc, VaultSvc	Servicios de Windows consultados durante la ejecución del exploit (Security Center, Program Compatibility Assistant, Credential Vault).

- **Mutexes creados**

TIPO	NOMBRE DEL MUTEX	DESCRIPCIÓN
Mutex global	Global_MSIExecute	Mutex relacionado con instalaciones MSI activas — consultado para detectar entornos de administración.
Mutex global	Global\AdobeCrashProcessorLocalLowLock	Mutex del procesador de crashs de Adobe — usado por el proceso de post-explotación.
Mutex global	Global\OneSettingQueryMutex+compat+encapsulation	Mutex de configuración del sistema — consultado durante el reconocimiento del entorno.

- **Árbol de procesos sospechoso**

El siguiente árbol de procesos fue observado en análisis de sandbox (CAPE / Zenbox) al abrir el PDF malicioso:

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

PROCESO	PID (REF.)	COMPORTAMIENTO OBSERVADO
Acrobat.exe (proceso raíz)	PID: 6416	Proceso principal que abre el archivo 'manual.pdf'. Dispara toda la cadena de ejecución del exploit.
└── AdobeCollabSync.exe -c	PID: 3520, 5424, 1376, 1428...	Proceso hijo generado múltiples veces (12+ instancias en Zenbox). El flag -c indica modo de configuración. Ejecución excesiva es indicador de compromiso. Etiquetado como PERSISTENCE en sandbox.
└── Adobe Crash Processor.exe	PID: 5784	Lee memoria de procesos remotos — comportamiento anómalo para este proceso.
└── CRWindowsClientService.exe	PID: 2956	Proceso hijo de nivel 3 — genera subprocesos adicionales de log (CRLogTransport.exe).
└── CRLogTransport.exe (x2)	PID: 5384, 5148	Transporte de logs — procesos terminales del árbol de ejecución.

Indicadores de Comportamiento

- Adobe Reader ejecutando conexiones de red salientes inesperadas.
- Apertura de streams de archivos locales sin acción explícita del usuario.
- Procesos hijo iniciados desde Acrobat/Reader hacia herramientas del sistema.
- Intentos de escritura en directorios del sistema desde el contexto de Adobe Reader.

Vulnerabilidades.

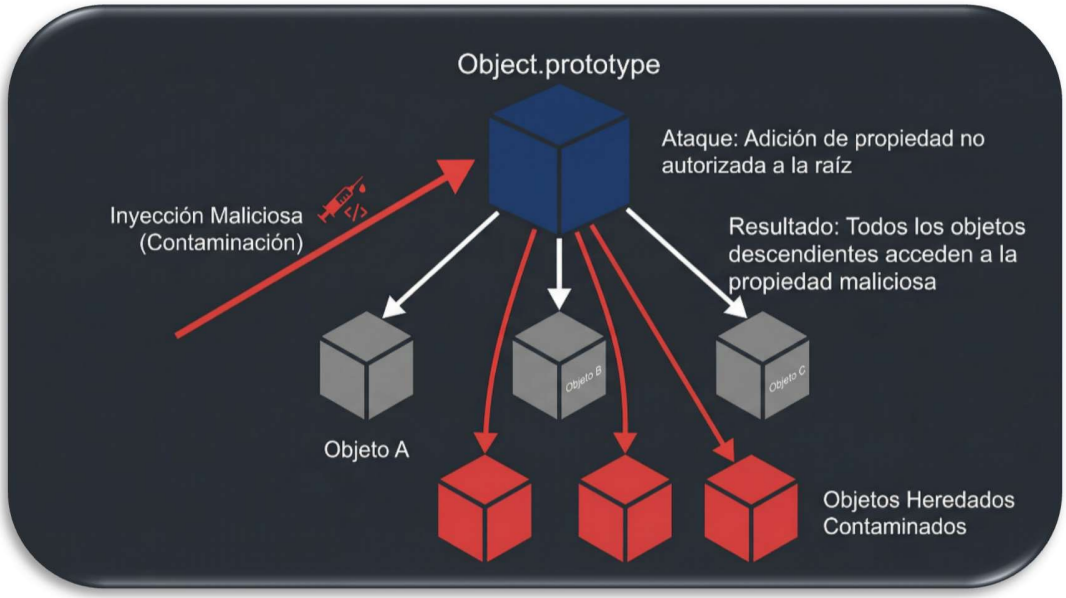
En JavaScript, cada objeto tiene internamente una referencia a un objeto prototipo del que hereda propiedades y métodos. El prototipo base de todos los objetos es Object.prototype. Cuando una aplicación no valida ni sanitiza correctamente las claves de propiedades que un usuario (o código externo) puede asignar en objetos, es posible que un atacante asigne valores a propiedades especiales como __proto__, constructor o prototype.

Al hacer esto, el atacante contamina Object.prototype: todos los objetos en la aplicación que hereden de él comenzarán a tener las propiedades maliciosas inyectadas. Esto puede alterar

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

la lógica de control de la aplicación, deshabilitar verificaciones de seguridad, cambiar valores de configuración esperados o desencadenar rutas de código no previstas que deriven en ejecución de código arbitrario.

Ejemplo conceptual del mecanismo de ataque: Si el motor JavaScript de Acrobat comprueba un valor como obj.isPrivileged antes de ejecutar una API privilegiada, y el atacante inyecta Object.prototype.isPrivileged = true mediante Prototype Pollution, todas las instancias de objetos en el runtime heredarán esa propiedad como true, eludiendo el control de acceso sin necesitar explotar ningún mecanismo adicional.



APIs privilegiadas de Adobe Acrobat involucradas

util.readFileIntoStream()	API de Acrobat que normalmente requiere contexto privilegiado. Permite leer el contenido de archivos del sistema de archivos local y convertirlo en un stream de datos. Mediante la adulteración del prototipo, el exploit la invoca sin restricciones del sandbox, exfiltrando archivos locales sensibles.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

RSS.addFeed()	API de Acrobat originalmente diseñada para gestión de feeds RSS. El exploit la usa para realizar peticiones HTTP a URLs controladas por el atacante, tanto para exfiltrar datos recopilados del sistema como para descargar y ejecutar código malicioso de segunda etapa.

Principales activos afectados.

Adobe ha publicado bajo el boletín APSB26-43 (11 de abril de 2026) la siguiente lista de versiones vulnerables y sus correspondientes correcciones:

PRODUCTO	VERSIONES AFECTADAS / CORREGIDAS	PLATAFORMA	ESTADO
Acrobat DC	26.001.21367 y anteriores	Win / macOS	VULNERABLE
Acrobat DC	26.001.21411	Win / macOS	CORREGIDO
Acrobat Reader DC	26.001.21367 y anteriores	Win / macOS	VULNERABLE
Acrobat Reader DC	26.001.21411	Win / macOS	CORREGIDO
Acrobat 2024	24.001.30356 y anteriores	Win / macOS	VULNERABLE
Acrobat 2024	24.001.30362 (Win) / 24.001.30360 (macOS)	Win / macOS	CORREGIDO

Nota importante: Adobe clasificó esta actualización con Prioridad 1 (P1), el nivel más alto de urgencia, lo que indica que el parche debe desplegarse en el menor tiempo posible, idealmente en un plazo no mayor a 24-72 horas desde su disponibilidad.

Recomendaciones

Remediación inmediata (PRIORIDAD CRÍTICA)

- Actualizar Adobe Acrobat Reader / Acrobat DC a las versiones corregidas publicadas bajo el boletín APSB26-43: Acrobat DC / Reader DC versión 26.001.21411 o Acrobat 2024 versiones 24.001.30362 (Win) / 24.001.30360 (macOS). Utilizar Help > Check for

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Updates en la aplicación o desplegar mediante herramientas de gestión corporativa (SCCM, AIP-GPO, Apple Remote Desktop, SSH en macOS).

- Deshabilitar JavaScript en Adobe Acrobat Reader como medida de mitigación temporal si el parche no puede aplicarse de inmediato: Edit > Preferences > JavaScript > desactivar 'Enable Acrobat JavaScript'. Esta acción reduce significativamente la superficie de ataque al impedir la ejecución del exploit.
- Bloquear en firewall y proxy corporativo todo tráfico HTTP/HTTPS que contenga el User-Agent 'Adobe Synchronizer' en el campo de cabecera, especialmente desde procesos de Adobe Reader hacia destinos externos no documentados.
- Restringir la apertura de archivos PDF adjuntos de fuentes no verificadas hasta que todos los endpoints institucionales hayan sido actualizados.

Detección activa

- Monitorear en el SIEM institucional la creación de procesos hijo inusuales desde acrobat.exe o AcroCEF.exe (cmd.exe, powershell.exe, wscript.exe, mshta.exe) usando reglas SIGMA o correlaciones de eventos de Windows Event ID 4688.
- Configurar reglas en el EDR para alertar sobre acceso a archivos fuera de rutas habituales iniciado desde procesos de Adobe Reader, incluyendo archivos en AppData, carpetas de credenciales del sistema o documentos de usuario masivos.
- Implementar detección de tráfico de red con el User-Agent 'Adobe Synchronizer' en el proxy y firewall perimetral, generando alertas para análisis inmediato.
- Enviar archivos PDF sospechosos recibidos por correo electrónico o descargados de fuentes externas a análisis en sandbox (como EXPMON, Any.run, Joe Sandbox) antes de su apertura en estaciones de trabajo institucionales.
- Revisar y actualizar las firmas de los motores antivirus instalados para incluir detección de las muestras PDF asociadas a CVE-2026-34621.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Hardening y buenas prácticas

- Aplicar el principio de mínimo privilegio: configurar las cuentas de usuario con las que opera el personal del sector salud sin privilegios de administrador local para limitar el impacto de una eventual explotación.
- Configurar reglas de AppLocker o Windows Defender Application Control (WDAC) para prevenir la ejecución de procesos no autorizados desde el directorio de Adobe Reader.
- Implementar filtrado avanzado de correo electrónico con capacidad de detonación de adjuntos en sandbox antes de entrega al buzón del usuario.
- Sensibilizar al personal de la institución sobre la no apertura de archivos PDF de remitentes desconocidos, especialmente aquellos que prometen información urgente de tipo clínico, administrativo o financiero.
- Mantener una política de actualización de software activa con verificación periódica de versiones instaladas de Adobe Acrobat en el inventario de activos (mínimo mensual).
- Activar la protección de vista protegida (Protected View) en Adobe Acrobat para todos los archivos procedentes de fuentes externas (Edit > Preferences > Security > Protected View > Files from potentially unsafe locations).

Reglas de red (Firewall / Proxy / IDS)

- BLOQUEAR toda comunicación HTTP/HTTPS con User-Agent que contenga: 'Adobe Synchronizer'
- ALERTAR sobre parámetros de URL: &od=422974 o &od=319988 en cualquier tráfico saliente
- ALERTAR sobre paths: /rs1?rnd=, /s11?language=, /s12?language=, /rs2 en tráfico desde procesos de Adobe
- BLOQUEAR conexiones TCP hacia 188.214.34.20 (todos los puertos, especialmente 34123)
- BLOQUEAR conexiones TCP hacia 169.40.2.68 (todos los puertos, especialmente 45191)
- BLOQUEAR dominio ado-read-parser.com y todos sus subdominios (*.ado-read-parser.com)

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

- ALERTAR sobre tráfico TCP desde procesos Acrobat.exe / AcroCEF.exe hacia puertos no estándar (>10000)
- DETECTAR JA3: cd08e31494f9531f560d64c695473da9 en conexiones TLS originadas desde Adobe Reader

Indicadores YARA (estructura PDF)

- Presencia simultánea en el PDF de: /AcroForm + /OpenAction + /JS con patrones JSFuck: ({}+[])[[+!+[]]]
- Campo de formulario oculto: /Rect [0 0 0 0] con /FT /Btn y /T (btn1)
- Strings decodificadas del payload: readFileIntoStream, addFeed, removeFeed, final_js
- Cadena de ejecución: eval(global.final_js)
- Variables animal-temáticas: dog1, dog2, bird0, bird1, pig0, deer, reindeer
- Marcadores de campaña: 422974, 319988
- Nombre de acción JS: PrintReport_54

Fuentes:

- Forbes / Davey Winder. "PDF Warning: Adobe Reader Zero-Day Attack Ongoing Since 2025." https://www.forbes.com/sites/daveywinder/2026/04/11/pdf-warning-adobe-reader-zero-day-attack-ongoing-since-2025/
- Adobe Security Bulletin. "APSB26-43 — Security update for Adobe Acrobat and Reader." https://helpx.adobe.com/security/products/acrobat/apsb26-43.html
- The Hacker News. "Adobe Reader Zero-Day Exploited via Malicious PDFs Since December 2025." https://thehackernews.com/2026/04/adobe-reader-zero-day-exploited-via.html
- The Hacker News. "Adobe Patches Actively Exploited Acrobat Reader Flaw CVE-2026-34621." https://thehackernews.com/2026/04/adobe-patches-actively-exploited.html
- Cyber Kendra. "Adobe Acrobat Zero-Day CVE-2026-34621 Under Active Attack." https://www.cyberkendra.com/2026/04/adobe-acrobat-zero-day-cve-2026-34621.html

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

- Born's Tech and Windows World. "Adobe Reader: Emergency patch for 0-day vulnerability CVE-2026-34621." https://borncity.com/win/2026/04/12/adobe-reader-emergency-patch-for-0-day-vulnerability-cve-2026-34621/
- GitHub Gist (N3mes1s). "Adobe Reader Zero-Day PDF Exploit — Full Forensic Analysis." https://gist.github.com/N3mes1s/9e55e8d781235ee256d5b3f6720222dd
- MITRE ATT&CK. "Enterprise Matrix — MITRE ATT&CK Framework." https://attack.mitre.org/
- NVD — NIST. "CVE-2026-34621 — National Vulnerability Database." https://nvd.nist.gov/vuln/detail/CVE-2026-34621

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el CSIRT Salud a través de las líneas telefónicas (+57) 3168931490 - 3181553570 o mediante el correo electrónico csirtsalud@minsalud.gov.co. Nuestro equipo está disponible para brindar el acompañamiento necesario.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570