

Alerta ID:	120
Fecha del reporte:	07/07/2026
Entidad:	Todas las entidades del ecosistema digital
Título:	Vulnerabilidad de Denegación de Servicio Remota (DoS) en PHP (CVE-2026-12184) puede ser explotada durante el establecimiento de conexiones TLS y afectar la disponibilidad de aplicaciones críticas utilizadas por organizaciones del sector salud.
Herramienta de detección	N/A
Activo involucrado:	Servidores web que ejecutan PHP, servidores Linux y Windows, aplicaciones web desarrolladas en PHP, portales institucionales, plataformas de Historia Clínica Electrónica (HCE), sistemas de información hospitalaria (HIS), sistemas RIS, PACS, LIS, plataformas de telemedicina, portales de resultados clínicos, aplicaciones de interoperabilidad clínica, APIs institucionales, servidores de autenticación, aplicaciones administrativas, soluciones ERP hospitalarias, servicios web expuestos mediante HTTPS, plataformas de interoperabilidad con terceros, infraestructura alojada en centros de datos institucionales y servicios desplegados en entornos de computación en la nube que utilicen versiones vulnerables de PHP.
Tipo de alerta:	Alerta
Nivel de riesgo:	Alto

Objetivo:

Informar a las organizaciones del sector salud en Colombia sobre la vulnerabilidad **CVE-2026-12184**, recientemente corregida por el Proyecto PHP, la cual permite que un servidor remoto especialmente preparado provoque condiciones de **Denegación de Servicio (Denial of Service – DoS)** durante el establecimiento de conexiones protegidas mediante **Transport Layer Security (TLS)**. La explotación de esta vulnerabilidad puede ocasionar la terminación inesperada de procesos que utilizan PHP para establecer comunicaciones cifradas con servicios

remotos, afectando la disponibilidad de aplicaciones críticas y generando interrupciones operativas sobre plataformas que soportan procesos asistenciales, administrativos y de interoperabilidad clínica.

La vulnerabilidad evidencia cómo errores presentes en componentes ampliamente utilizados por aplicaciones empresariales pueden ser aprovechados por actores de amenaza para afectar la continuidad de los servicios sin necesidad de ejecutar código arbitrario sobre el servidor comprometido. Aunque el impacto identificado corresponde principalmente a la disponibilidad, la indisponibilidad de aplicaciones críticas representa un riesgo significativo para organizaciones cuya operación depende del intercambio permanente de información mediante canales seguros.

El propósito de esta alerta es que las entidades evalúen el impacto potencial que esta vulnerabilidad podría generar sobre:

- servidores web que ejecutan aplicaciones desarrolladas en PHP;
- plataformas de Historia Clínica Electrónica (HCE);
- aplicaciones de telemedicina;
- sistemas de información hospitalaria (HIS);
- plataformas RIS y PACS utilizadas para diagnóstico por imágenes;
- sistemas de laboratorio clínico (LIS);
- portales institucionales de atención al ciudadano;
- aplicaciones administrativas y financieras;
- servicios de autenticación corporativa;
- APIs utilizadas para interoperabilidad con terceros;
- servicios web publicados mediante HTTPS;
- plataformas de integración con proveedores externos;
- infraestructura tecnológica desplegada en ambientes físicos, virtuales y en la nube.

En el sector salud, donde una parte importante de los procesos asistenciales depende del acceso continuo a aplicaciones web y servicios interoperables, la indisponibilidad ocasionada por la explotación de esta vulnerabilidad podría afectar la continuidad operacional, retrasar procesos clínicos, interrumpir servicios de atención, impedir el intercambio oportuno de información médica y aumentar la carga operativa de los equipos responsables de tecnología, continuidad del negocio y ciberseguridad. Por este motivo, resulta fundamental que las

organizaciones identifiquen oportunamente los activos expuestos, validen las versiones de PHP actualmente instaladas e implementen las actualizaciones de seguridad publicadas por el fabricante con el fin de reducir el riesgo de afectación operacional.

Descripción:

El Proyecto PHP publicó recientemente actualizaciones de seguridad destinadas a corregir la vulnerabilidad **CVE-2026-12184**, identificada durante el procesamiento de conexiones seguras establecidas mediante **Transport Layer Security (TLS)**. La vulnerabilidad puede ser explotada por un servidor remoto especialmente preparado para provocar una condición de **Denegación de Servicio (DoS)** durante la negociación criptográfica, ocasionando la finalización inesperada del proceso que realiza la conexión o la interrupción del servicio asociado.

A diferencia de vulnerabilidades orientadas a la ejecución remota de código, elevación de privilegios o divulgación de información, este escenario afecta principalmente la **disponibilidad** de las aplicaciones desarrolladas sobre PHP. La explotación ocurre cuando una aplicación vulnerable intenta establecer una conexión TLS hacia un servidor remoto controlado por un actor de amenaza. Durante el intercambio inicial de mensajes del protocolo, el servidor responde con datos especialmente contruidos que desencadenan una condición de error capaz de finalizar el proceso responsable de la comunicación segura.

Desde una perspectiva técnica, la vulnerabilidad se presenta durante la gestión de determinadas condiciones excepcionales asociadas al establecimiento de sesiones TLS. Un actor malicioso que controle un servidor remoto puede manipular la respuesta enviada durante la negociación criptográfica para provocar fallos internos en el componente que administra la conexión, generando la interrupción del proceso sin necesidad de comprometer directamente el sistema operativo, modificar archivos locales o ejecutar código arbitrario sobre el servidor afectado.

Este comportamiento convierte la disponibilidad en el principal objetivo del ataque. Dependiendo de la arquitectura implementada por la organización, una aplicación vulnerable podría experimentar interrupciones repetitivas cuando establezca comunicaciones con servicios externos especialmente preparados para explotar la vulnerabilidad. En entornos donde múltiples procesos automatizados dependen continuamente de conexiones TLS, un atacante

podría generar fallos recurrentes que afecten la estabilidad general de la aplicación y degraden progresivamente la prestación del servicio.

En organizaciones del sector salud, donde numerosas plataformas intercambian información mediante servicios web protegidos con TLS, el impacto potencial adquiere una relevancia considerable. Aplicaciones relacionadas con Historia Clínica Electrónica, interoperabilidad clínica, sistemas de laboratorio, plataformas RIS, PACS, telemedicina, autenticación federada, correo institucional, servicios de identidad digital e integración con entidades externas utilizan permanentemente conexiones seguras para garantizar la confidencialidad e integridad de la información transmitida. La interrupción de dichas comunicaciones puede afectar procesos clínicos y administrativos cuya continuidad resulta esencial para la prestación de servicios de salud.

Adicionalmente, la vulnerabilidad demuestra la importancia de mantener actualizados los componentes base sobre los cuales operan múltiples aplicaciones institucionales. PHP continúa siendo uno de los lenguajes de programación más utilizados para el desarrollo de aplicaciones empresariales y portales web. Como consecuencia, una vulnerabilidad presente en su mecanismo de comunicación segura puede impactar simultáneamente numerosos servicios críticos que dependen de la misma plataforma tecnológica.

Aunque actualmente no existe evidencia pública que indique campañas masivas de explotación dirigidas contra organizaciones del sector salud, la divulgación técnica de la vulnerabilidad incrementa la probabilidad de que actores de amenaza desarrollen herramientas automatizadas destinadas a identificar servidores vulnerables y provocar interrupciones deliberadas de los servicios expuestos. Este escenario resulta especialmente relevante para entidades que mantienen aplicaciones accesibles desde Internet o que establecen comunicaciones frecuentes con múltiples servicios externos.

Por lo anterior, el CSIRT Salud recomienda que todas las organizaciones del sector identifiquen los activos que ejecutan versiones vulnerables de PHP, validen la exposición de aplicaciones que establezcan conexiones TLS con servicios remotos y prioricen la implementación de las actualizaciones de seguridad publicadas por el Proyecto PHP como parte de sus procesos de gestión de vulnerabilidades y continuidad del negocio.

Consecuencias de la explotación



La explotación exitosa de la vulnerabilidad **CVE-2026-12184** puede generar impactos significativos sobre la disponibilidad de aplicaciones críticas, la continuidad operacional de los servicios institucionales y la estabilidad de las plataformas tecnológicas que utilizan PHP para establecer comunicaciones protegidas mediante **Transport Layer Security (TLS)**. Aunque la vulnerabilidad no permite la ejecución remota de código, la elevación de privilegios ni el acceso directo a información almacenada en los sistemas afectados, su capacidad para interrumpir procesos asociados a conexiones seguras representa un escenario de riesgo relevante para organizaciones cuya operación depende del intercambio permanente de información con servicios externos.

Uno de los principales impactos corresponde a la interrupción inesperada de procesos que establecen conexiones TLS hacia servidores remotos. Cuando una aplicación vulnerable inicia una sesión segura con un servidor especialmente preparado para explotar la vulnerabilidad, la negociación criptográfica puede desencadenar una condición de error que ocasiona la finalización del proceso responsable de la comunicación. Dependiendo de la arquitectura implementada por la organización, esta situación puede traducirse en la indisponibilidad parcial o total de funcionalidades críticas soportadas por la aplicación.

Desde una perspectiva operacional, la afectación puede extenderse más allá del proceso inicialmente comprometido. Numerosas aplicaciones desarrolladas sobre PHP implementan arquitecturas basadas en microservicios, servicios web, APIs REST, plataformas de interoperabilidad o integraciones con proveedores externos. La interrupción repetitiva de las conexiones TLS puede generar fallos en cascada sobre procesos dependientes, ocasionando degradación del rendimiento, incremento de tiempos de respuesta, errores durante la sincronización de información y pérdida temporal de funcionalidades esenciales para la operación institucional.

En organizaciones del sector salud, donde las aplicaciones clínicas intercambian permanentemente información con múltiples plataformas internas y externas, este escenario adquiere una importancia particular. Sistemas de Historia Clínica Electrónica (HCE), plataformas de telemedicina, aplicaciones de laboratorio clínico (LIS), sistemas RIS, plataformas PACS, servicios de autenticación federada, portales para pacientes, sistemas

administrativos, soluciones financieras y plataformas de interoperabilidad utilizan conexiones TLS para garantizar la confidencialidad e integridad de la información transmitida. La indisponibilidad de estos mecanismos de comunicación puede afectar directamente la continuidad de procesos asistenciales y administrativos.

Otro impacto relevante corresponde a la degradación progresiva de los servicios cuando la vulnerabilidad es explotada de forma repetitiva. Un actor de amenaza podría inducir múltiples intentos de conexión hacia servidores controlados, provocando fallos sucesivos sobre los procesos vulnerables. Dependiendo de la configuración de la aplicación, estos eventos pueden ocasionar reinicios continuos, incremento del consumo de recursos, generación masiva de registros de error, agotamiento de procesos disponibles o interrupciones prolongadas mientras los mecanismos automáticos de recuperación intentan restablecer el servicio.

La explotación de esta vulnerabilidad también puede afectar los mecanismos de interoperabilidad implementados entre entidades del sector salud. Diversas organizaciones mantienen conexiones permanentes con plataformas gubernamentales, aseguradores, laboratorios de referencia, proveedores tecnológicos, sistemas de autenticación y servicios alojados en la nube. Cuando alguno de estos procesos depende de componentes vulnerables, la interrupción de las comunicaciones puede retrasar el intercambio de información clínica, afectar la disponibilidad de resultados diagnósticos, impedir procesos de autenticación o limitar temporalmente la prestación de servicios digitales dirigidos a pacientes y profesionales de la salud.

Desde la perspectiva de continuidad del negocio, una condición prolongada de Denegación de Servicio puede obligar a las organizaciones a activar procedimientos internos de contingencia, utilizar procesos manuales, suspender temporalmente determinadas funcionalidades o redirigir la operación hacia infraestructuras alternas. Aunque estas medidas permiten mantener parcialmente la prestación del servicio, incrementan significativamente la carga operativa de las áreas de tecnología, soporte y ciberseguridad, además de aumentar el riesgo de errores derivados de la ejecución manual de actividades previamente automatizadas.

Otro aspecto que debe considerarse corresponde al impacto sobre los acuerdos de niveles de servicio (SLA). La indisponibilidad de aplicaciones expuestas a esta vulnerabilidad puede afectar compromisos establecidos con usuarios, entidades externas, proveedores tecnológicos y organismos del sector salud. En escenarios donde múltiples aplicaciones compartan la misma

infraestructura PHP, la explotación de la vulnerabilidad podría generar interrupciones simultáneas sobre diferentes servicios institucionales, amplificando considerablemente el impacto operacional.

La divulgación pública de la vulnerabilidad incrementa además el riesgo de explotación oportunista. Una vez disponibles los detalles técnicos y las actualizaciones de seguridad, es habitual que actores maliciosos desarrollen herramientas automatizadas destinadas a identificar servidores vulnerables mediante procesos de reconocimiento masivo. Aunque la vulnerabilidad requiere condiciones específicas para su explotación, la disponibilidad de información técnica reduce significativamente el esfuerzo necesario para incorporar este tipo de ataques dentro de campañas automatizadas dirigidas contra servicios expuestos a Internet. En infraestructuras hospitalarias modernas, donde numerosos servicios funcionan de manera ininterrumpida las veinticuatro horas del día, cualquier interrupción sobre aplicaciones clínicas puede generar efectos acumulativos sobre la atención de pacientes.

La indisponibilidad temporal de portales clínicos, sistemas de interoperabilidad o plataformas de autenticación puede retrasar la consulta de información médica, afectar procesos administrativos, limitar el acceso a resultados diagnósticos y generar congestión en otros sistemas institucionales que dependen de dichos servicios para operar correctamente.

Adicionalmente, los eventos asociados a esta vulnerabilidad pueden incrementar considerablemente la carga de trabajo de los equipos responsables de monitoreo, respuesta a incidentes y administración de infraestructura. La generación continua de errores relacionados con conexiones TLS puede dificultar la identificación temprana de otras actividades maliciosas, incrementar el volumen de alertas registradas por herramientas de monitoreo y prolongar el tiempo requerido para realizar análisis de causa raíz, especialmente en entornos donde múltiples aplicaciones comparten componentes tecnológicos comunes.

En escenarios donde la vulnerabilidad sea utilizada como parte de campañas de ataque más amplias, una condición inicial de Denegación de Servicio podría emplearse para distraer a los equipos responsables de la operación mientras se desarrollan actividades adicionales de reconocimiento, explotación de otras vulnerabilidades o ataques dirigidos contra diferentes componentes de la infraestructura tecnológica. Aunque actualmente no existen evidencias públicas que asocien la vulnerabilidad con este tipo de campañas, la indisponibilidad de

servicios críticos puede convertirse en un elemento facilitador para otras fases del ciclo de ataque.

En escenarios de explotación exitosa, un actor de amenaza podría:

- provocar la terminación inesperada de procesos que establecen conexiones TLS mediante PHP;
- afectar la disponibilidad de aplicaciones web críticas utilizadas por la organización;
- interrumpir procesos de interoperabilidad con plataformas externas;
- generar degradación progresiva del rendimiento de aplicaciones dependientes de conexiones seguras;
- incrementar el consumo de recursos asociados a mecanismos automáticos de recuperación de servicios;
- afectar temporalmente plataformas de Historia Clínica Electrónica, telemedicina, RIS, PACS y sistemas de laboratorio que dependan de componentes vulnerables;
- ocasionar indisponibilidad de servicios institucionales publicados mediante HTTPS;
- aumentar la carga operativa de los equipos responsables de infraestructura, continuidad del negocio y ciberseguridad;
- afectar el cumplimiento de acuerdos de niveles de servicio establecidos con usuarios y proveedores;
- facilitar escenarios de interrupción operacional que puedan ser aprovechados durante campañas de ataque más amplias dirigidas contra la infraestructura tecnológica institucional.

Aunque **CVE-2026-12184** no incorpora capacidades orientadas al robo de información, ejecución remota de código o establecimiento de persistencia sobre los sistemas afectados, la interrupción de servicios críticos continúa representando un riesgo significativo para organizaciones cuya operación depende del funcionamiento continuo de aplicaciones desarrolladas sobre PHP.

Modo de explotación del ataque

Fase 1 – Reconocimiento e identificación de aplicaciones PHP expuestas

La cadena de ataque inicia con actividades de reconocimiento orientadas a identificar aplicaciones desarrolladas sobre PHP que establezcan conexiones TLS hacia servicios remotos. A diferencia de otras campañas que requieren comprometer inicialmente el servidor objetivo, la explotación de CVE-2026-12184 depende de identificar aplicaciones que actúen como clientes durante el establecimiento de comunicaciones seguras. En consecuencia, los actores de amenaza realizan actividades de enumeración con el propósito de identificar plataformas que consuman servicios externos mediante HTTPS, Web Services, APIs REST, SOAP, LDAP sobre TLS (LDAPS), SMTPS, IMAPS, POP3S u otros protocolos protegidos mediante TLS.

Durante esta fase, el reconocimiento puede desarrollarse utilizando fuentes abiertas de información (OSINT), motores de búsqueda especializados para activos expuestos, plataformas de reconocimiento automatizado, análisis de certificados digitales, revisión de encabezados HTTP, fingerprinting de tecnologías web y consultas sobre registros DNS públicos. Estas actividades permiten determinar la presencia de aplicaciones desarrolladas sobre PHP, identificar versiones potencialmente vulnerables y establecer relaciones entre diferentes servicios publicados por la organización.

Los actores de amenaza también pueden realizar reconocimiento pasivo mediante el análisis de certificados X.509, registros WHOIS, servicios de transparencia de certificados (Certificate Transparency Logs), información publicada por motores de búsqueda especializados y repositorios públicos donde se evidencien tecnologías utilizadas por la organización. En escenarios más avanzados, el reconocimiento puede complementarse con la enumeración de rutas de aplicaciones, identificación de frameworks PHP, análisis de respuestas HTTP y observación del comportamiento de aplicaciones durante el establecimiento de conexiones hacia servicios externos.

En organizaciones del sector salud, esta etapa puede revelar la existencia de plataformas de Historia Clínica Electrónica (HCE), portales para pacientes, aplicaciones de telemedicina, servicios de interoperabilidad clínica, plataformas de autenticación, aplicaciones administrativas, sistemas de laboratorio, soluciones RIS/PACS y portales institucionales

desarrollados sobre PHP que mantienen comunicaciones permanentes con múltiples servicios externos mediante conexiones TLS.

Las actividades realizadas durante esta fase pueden incluir:

- identificación de aplicaciones desarrolladas sobre PHP expuestas a Internet;
- fingerprinting de tecnologías utilizadas por servidores web;
- identificación de servicios que establecen conexiones TLS hacia terceros;
- recopilación de información mediante técnicas OSINT;
- análisis de certificados digitales publicados;
- identificación de frameworks y componentes utilizados por las aplicaciones;
- elaboración del inventario de objetivos potencialmente vulnerables.

El objetivo consiste en identificar aplicaciones PHP que establezcan conexiones TLS con servicios remotos y determinar aquellas que podrían ser susceptibles de explotación mediante la vulnerabilidad CVE-2026-12184.

Fase 2 – Preparación de la infraestructura controlada por el actor de amenaza

Una vez identificadas las aplicaciones objetivo, el actor de amenaza prepara la infraestructura que utilizará para inducir la condición vulnerable. A diferencia de un servidor TLS convencional, el servidor malicioso implementa un comportamiento específicamente diseñado para responder de manera anómala durante el proceso de negociación criptográfica. Esta infraestructura puede consistir en servidores propios, servicios alojados en la nube, sistemas previamente comprometidos o plataformas temporales desplegadas exclusivamente para la ejecución del ataque.

Desde una perspectiva técnica, el servidor es configurado para manipular la secuencia de mensajes intercambiados durante el TLS Handshake, generando respuestas especialmente construidas que provocan condiciones inesperadas dentro del componente responsable de procesar la conexión segura en PHP. Dependiendo de la implementación utilizada, estas respuestas pueden incorporar secuencias de mensajes incompletas, estructuras inconsistentes o eventos que desencadenan errores durante el procesamiento interno de la sesión criptográfica.

En campañas más sofisticadas, la infraestructura maliciosa puede distribuirse geográficamente mediante múltiples servidores para incrementar la disponibilidad del ataque, dificultar su bloqueo y permitir la explotación simultánea de diferentes aplicaciones vulnerables pertenecientes a múltiples organizaciones.

Las actividades realizadas durante esta fase pueden incluir:

- despliegue de servidores TLS controlados por el atacante;
- configuración de respuestas específicamente diseñadas para activar la vulnerabilidad;
- preparación de certificados digitales utilizados durante la negociación;
- validación del comportamiento del servidor frente a clientes PHP vulnerables;
- automatización del proceso de explotación;
- distribución geográfica de la infraestructura utilizada durante el ataque;
- verificación del funcionamiento del entorno antes del inicio de la explotación.

El objetivo consiste en disponer de un servidor capaz de inducir condiciones anómalas durante la negociación TLS con aplicaciones PHP vulnerables.

Fase 3 – Establecimiento de la conexión TLS

Una vez preparada la infraestructura, el ataque inicia cuando la aplicación vulnerable intenta establecer una conexión segura con el servidor remoto controlado por el actor de amenaza. Esta situación puede producirse como consecuencia de procesos completamente legítimos desarrollados por la propia aplicación, incluyendo consultas a APIs externas, servicios de autenticación, sincronización de información clínica, consumo de servicios SOAP o REST, integración con proveedores tecnológicos o comunicaciones automatizadas programadas por la organización.

Durante esta etapa, el cliente PHP inicia el proceso normal de negociación TLS enviando el mensaje ClientHello, indicando los algoritmos criptográficos soportados, versiones del protocolo, extensiones habilitadas y demás parámetros necesarios para establecer el canal seguro. Hasta este momento, la comunicación se desarrolla conforme al comportamiento esperado por el protocolo TLS.

El servidor controlado por el atacante responde posteriormente utilizando una secuencia de mensajes diseñada específicamente para activar la condición vulnerable presente en la implementación afectada de PHP. La explotación ocurre durante el procesamiento interno de dicha respuesta, antes de que la sesión criptográfica alcance un estado operativo.

Las actividades realizadas durante esta fase pueden incluir:

- establecimiento de conexiones HTTPS hacia servidores controlados;
- inicio del proceso TLS Handshake;
- intercambio inicial de mensajes criptográficos;
- negociación de algoritmos de cifrado;
- procesamiento de certificados digitales;
- recepción de respuestas especialmente construidas;
- activación del flujo vulnerable durante la negociación.

El objetivo consiste en inducir a la aplicación vulnerable a procesar una respuesta TLS especialmente diseñada para activar la condición de fallo.

Fase 4 – Activación de la condición de Denegación de Servicio

Una vez procesada la respuesta enviada por el servidor remoto, la implementación vulnerable de PHP entra en una condición de error durante la gestión de la sesión TLS. Dependiendo de la arquitectura utilizada por la aplicación, el comportamiento resultante puede incluir la terminación inesperada del proceso, la interrupción del flujo de comunicación, excepciones no controladas, finalización del worker responsable de atender la solicitud o el cierre abrupto de la conexión.

Desde una perspectiva operacional, el fallo puede manifestarse de diferentes maneras según el servidor web utilizado (Apache HTTP Server, Nginx con PHP-FPM u otras implementaciones), la configuración del gestor de procesos y los mecanismos internos de recuperación implementados por la organización. En entornos de alta concurrencia, la repetición del ataque puede afectar simultáneamente múltiples procesos de trabajo, reduciendo progresivamente la capacidad de atención del servicio.

Las actividades realizadas durante esta fase pueden incluir:

- procesamiento de mensajes TLS especialmente contruidos;
- activación de la condición vulnerable;
- generación de excepciones internas;
- terminación inesperada de procesos PHP;
- interrupción del flujo de comunicación cifrada;
- liberación anómala de recursos;
- indisponibilidad temporal del servicio asociado.

El objetivo consiste en provocar la interrupción del proceso responsable de la comunicación segura y afectar la disponibilidad de la aplicación vulnerable.

Fase 5 – Degradación operacional y afectación de servicios institucionales

Una vez producida la condición de Denegación de Servicio, los efectos comienzan a propagarse hacia los procesos dependientes de la aplicación afectada. La indisponibilidad de conexiones TLS puede impedir el intercambio de información con servicios externos, afectar procesos automatizados de interoperabilidad y generar errores sucesivos en componentes que dependen de dichas comunicaciones para completar su operación normal.

En organizaciones del sector salud, esta situación puede impactar procesos relacionados con Historia Clínica Electrónica, autenticación de usuarios, integración con plataformas nacionales, consulta de resultados diagnósticos, telemedicina, interoperabilidad clínica y otros servicios críticos cuya disponibilidad resulta indispensable para garantizar la continuidad de la atención. Las actividades realizadas durante esta fase pueden incluir:

- interrupción de servicios institucionales;
- fallos en procesos de interoperabilidad;
- degradación del rendimiento de aplicaciones;
- incremento del volumen de errores registrados;
- activación de mecanismos automáticos de recuperación;
- afectación de procesos clínicos y administrativos;

El objetivo consiste en maximizar el impacto operacional derivado de la interrupción de las comunicaciones TLS y afectar la continuidad de los servicios soportados por la aplicación vulnerable.

Fase 6 – Recuperación automática del servicio, persistencia de la indisponibilidad y evasión de mecanismos operacionales

Después de producirse la terminación anómala del proceso responsable de la conexión TLS, la infraestructura tecnológica puede iniciar mecanismos automáticos de recuperación implementados por PHP-FPM, Apache HTTP Server, Nginx, supervisores de procesos o plataformas de orquestación como Kubernetes. Aunque estos mecanismos permiten restablecer temporalmente el servicio, un actor de amenaza puede provocar nuevamente la condición vulnerable cada vez que la aplicación intente establecer una nueva conexión hacia el servidor controlado.

Desde una perspectiva técnica, el ataque no requiere mantener una sesión persistente con el servidor objetivo. Basta con responder repetidamente a las nuevas solicitudes TLS generadas por la aplicación para provocar sucesivas interrupciones de los procesos. En consecuencia, los mecanismos de recuperación automática pueden convertirse involuntariamente en un factor que prolongue la indisponibilidad operacional cuando la aplicación continúa intentando establecer conexiones con el mismo destino remoto.

En arquitecturas con balanceadores de carga, múltiples instancias PHP-FPM o entornos de alta disponibilidad, la explotación repetitiva puede distribuir el impacto entre diferentes nodos, incrementando el consumo de recursos, generando reinicios continuos de procesos y dificultando la identificación de la causa raíz del incidente. Dependiendo del monitoreo implementado por la organización, el comportamiento puede interpretarse inicialmente como una falla operacional o un problema de estabilidad de la aplicación.

Las actividades realizadas durante esta fase pueden incluir:

- reinicio automático de procesos PHP afectados;
- restablecimiento de workers por parte de PHP-FPM;
- nuevos intentos automáticos de conexión TLS;

- explotación repetitiva del mismo flujo vulnerable;
- incremento del consumo de CPU y memoria asociado a procesos de recuperación;

El objetivo consiste en mantener la condición de Denegación de Servicio durante el mayor tiempo posible, aprovechando los mecanismos automáticos de recuperación implementados por la infraestructura tecnológica.

Fase 7 – Impacto sobre la continuidad operacional y posible utilización dentro de campañas de ataque más amplias

Una vez consolidada la afectación sobre la disponibilidad de la aplicación, los actores de amenaza pueden aprovechar la indisponibilidad generada para incrementar el impacto operacional de otras actividades ofensivas. Aunque la vulnerabilidad CVE-2026-12184 no proporciona capacidades para ejecutar código, comprometer credenciales o establecer persistencia sobre los sistemas afectados, la interrupción de servicios críticos puede reducir temporalmente la capacidad de respuesta de la organización y favorecer la ejecución de campañas paralelas dirigidas contra otros componentes de la infraestructura tecnológica.

En organizaciones del sector salud, donde la continuidad de los servicios digitales constituye un elemento esencial para la atención de pacientes, la indisponibilidad de plataformas desarrolladas sobre PHP puede obligar a activar procedimientos de contingencia, ejecutar procesos manuales, utilizar infraestructuras alternas y destinar recursos adicionales para la recuperación del servicio. Estas actividades incrementan la carga operativa de los equipos de tecnología, continuidad del negocio y ciberseguridad, reduciendo su capacidad para responder simultáneamente a otros eventos de seguridad.

Desde una perspectiva estratégica, este tipo de vulnerabilidades evidencia cómo una condición limitada a la disponibilidad puede generar efectos operacionales de amplio alcance cuando afecta componentes tecnológicos ampliamente utilizados dentro de la organización. En consecuencia, la gestión oportuna de vulnerabilidades, el monitoreo continuo de componentes críticos y la aplicación temprana de actualizaciones de seguridad constituyen elementos fundamentales para fortalecer la resiliencia cibernética institucional.

Las actividades realizadas durante esta fase pueden incluir:

- interrupción prolongada de servicios institucionales;
- activación de planes de contingencia tecnológica;
- incremento de la carga operativa de los equipos de soporte;
- degradación de procesos asistenciales y administrativos;
- afectación del cumplimiento de acuerdos de nivel de servicio;
- utilización de la indisponibilidad como facilitador de otras actividades ofensivas;
- recuperación gradual de la operación mediante la aplicación de medidas correctivas.

El objetivo consiste en maximizar el impacto operacional derivado de la indisponibilidad de servicios críticos y aprovechar la interrupción para favorecer campañas de ataque de mayor alcance.

Vulnerabilidades asociadas



Procesamiento inadecuado durante el establecimiento de conexiones TLS

- **Descripción:** La vulnerabilidad CVE-2026-12184 se origina durante el procesamiento de determinadas condiciones asociadas al establecimiento de conexiones seguras mediante Transport Layer Security (TLS). Una aplicación desarrollada sobre PHP que inicia una comunicación cifrada con un servidor remoto especialmente preparado puede recibir respuestas diseñadas para provocar una condición de error durante la negociación criptográfica. Como consecuencia, el proceso responsable de establecer la conexión puede finalizar de manera inesperada, afectando la disponibilidad del servicio que realiza la comunicación.

El escenario demuestra cómo errores presentes en el manejo interno de protocolos criptográficos pueden convertirse en un vector de Denegación de Servicio cuando un actor de amenaza controla el comportamiento del servidor remoto durante el intercambio inicial de mensajes TLS.

- **Impacto:** La explotación exitosa puede provocar la terminación inesperada de procesos PHP, afectar la disponibilidad de aplicaciones críticas, interrumpir comunicaciones protegidas mediante TLS y degradar la continuidad operacional de plataformas que dependen del intercambio permanente de información con servicios externos.

- **Referencias técnicas:**
 - o MITRE ATT&CK: T1499 – Endpoint Denial of Service
 - o CWE: CWE-755 – Improper Handling of Exceptional Conditions

Gestión insuficiente de condiciones excepcionales durante la negociación criptográfica

- **Descripción:** La vulnerabilidad evidencia deficiencias en la gestión de condiciones excepcionales producidas durante la negociación TLS. Cuando una aplicación procesa respuestas inesperadas provenientes del servidor remoto, determinados estados internos pueden no ser gestionados adecuadamente, ocasionando la interrupción del flujo normal de ejecución. Este tipo de comportamiento incrementa la probabilidad de que eventos anómalos derivados de la comunicación provoquen condiciones de indisponibilidad.

Aunque la negociación TLS incorpora mecanismos destinados a garantizar la confidencialidad e integridad de las comunicaciones, la incorrecta administración de eventos excepcionales puede afectar la estabilidad del software encargado de implementar dichos mecanismos.

- **Impacto:** Las aplicaciones vulnerables pueden experimentar fallos repetitivos durante el establecimiento de conexiones seguras, generando indisponibilidad de servicios, reinicio continuo de procesos y degradación progresiva del rendimiento operacional.
- **Referencias técnicas:**
 - o MITRE ATT&CK: T1499 – Endpoint Denial of Service
 - o CWE: CWE-248 – Uncaught Exception

Dependencia de servicios externos mediante conexiones TLS

- **Descripción:** Las aplicaciones modernas desarrolladas sobre PHP suelen establecer comunicaciones continuas con servicios externos para autenticación, interoperabilidad, intercambio de información clínica, servicios en la nube, plataformas de correo electrónico, APIs REST y múltiples componentes distribuidos. Esta dependencia incrementa la superficie de exposición frente a vulnerabilidades que afectan el proceso de establecimiento de conexiones seguras.

En organizaciones del sector salud, una única aplicación puede mantener simultáneamente decenas de conexiones TLS hacia servicios críticos utilizados durante la atención de pacientes. Como consecuencia, la interrupción de cualquiera de estos canales puede generar efectos operacionales sobre procesos clínicos y administrativos.

- **Impacto:** La indisponibilidad de conexiones TLS puede afectar procesos de interoperabilidad, autenticación, sincronización de información clínica y funcionamiento de plataformas institucionales críticas.
- **Referencias técnicas:**
 - o MITRE ATT&CK: T1499 – Endpoint Denial of Service
 - o CWE: CWE-400 – Uncontrolled Resource Consumption

Ausencia de una gestión oportuna de vulnerabilidades

- **Descripción:** La explotación de CVE-2026-12184 resulta considerablemente más probable cuando las organizaciones mantienen versiones de PHP que ya cuentan con actualizaciones de seguridad publicadas por el fabricante. La ausencia de procesos formales de identificación, evaluación y remediación de vulnerabilidades incrementa el período durante el cual los sistemas permanecen expuestos frente a amenazas conocidas.

La gestión continua de vulnerabilidades constituye uno de los controles fundamentales para reducir la superficie de ataque y limitar la exposición frente a vulnerabilidades divulgadas públicamente.

- **Impacto:** La permanencia de versiones vulnerables facilita la explotación por parte de actores de amenaza, incrementa el riesgo de interrupción operacional y prolonga la exposición de servicios críticos utilizados por la organización.
- **Referencias técnicas:**
 - o MITRE ATT&CK: T1190 – Exploit Public-Facing Application
 - o CWE: CWE-1104 – Use of Unmaintained Third-Party Components

Deficiencias en el monitoreo de eventos asociados a conexiones TLS

- **Descripción:** La detección temprana de intentos de explotación depende en gran medida de la capacidad de las organizaciones para supervisar el comportamiento de las conexiones TLS establecidas por sus aplicaciones. La ausencia de monitoreo sobre errores de negociación criptográfica, reinicios inesperados de procesos PHP, fallos repetitivos de conexión y eventos asociados a servicios HTTPS puede retrasar significativamente la identificación de actividades maliciosas orientadas a provocar Denegación de Servicio.

Las organizaciones que carecen de mecanismos de correlación entre registros del servidor web, PHP-FPM, sistemas operativos, balanceadores de carga y plataformas SIEM presentan mayores dificultades para identificar patrones anómalos relacionados con este tipo de vulnerabilidades.

- **Impacto:** La detección tardía puede prolongar la indisponibilidad de aplicaciones críticas, incrementar el tiempo medio de respuesta (MTTR) y dificultar la ejecución de acciones de contención antes de que el impacto operacional se extienda hacia otros servicios institucionales.
- **Referencias técnicas:**
 - o MITRE ATT&CK: T1499 – Endpoint Denial of Service
 - o CWE: CWE-778 – Insufficient Logging

Infraestructura crítica dependiente de componentes compartidos

- **Descripción:** En numerosas organizaciones del sector salud, múltiples aplicaciones institucionales utilizan la misma versión de PHP, comparten servidores web, componentes criptográficos y plataformas de ejecución comunes. Esta arquitectura incrementa el impacto potencial de vulnerabilidades presentes en componentes base, debido a que un único fallo puede afectar simultáneamente diversos servicios críticos utilizados por diferentes áreas de la organización.

La utilización de componentes compartidos constituye una práctica habitual para simplificar la administración tecnológica; sin embargo, también amplifica el alcance de

vulnerabilidades cuando no existen mecanismos adecuados de segmentación, actualización y gestión del riesgo.

- **Impacto:** La explotación puede afectar simultáneamente múltiples aplicaciones institucionales, incrementar la indisponibilidad de servicios clínicos y administrativos, dificultar las actividades de recuperación y aumentar significativamente el impacto operacional sobre la organización.
- **Referencias técnicas:**
 - o MITRE ATT&CK: T1499 – Endpoint Denial of Service
 - o CWE: CWE-664 – Improper Control of a Resource Through its Lifetime

Recomendaciones

Las organizaciones del sector salud deben fortalecer los controles de seguridad implementados sobre la infraestructura tecnológica que soporta aplicaciones desarrolladas en PHP, con el propósito de reducir el riesgo asociado a la explotación de la vulnerabilidad **CVE-2026-12184**. Aunque la vulnerabilidad afecta principalmente la disponibilidad de los servicios durante el establecimiento de conexiones TLS, su impacto puede extenderse hacia procesos asistenciales y administrativos cuya operación depende del intercambio continuo de información mediante canales seguros. En consecuencia, el CSIRT Salud recomienda adoptar las siguientes medidas preventivas y de fortalecimiento de la postura de ciberseguridad.

Actualizar inmediatamente las versiones vulnerables de PHP

Las organizaciones deben identificar todos los servidores que ejecutan versiones vulnerables de PHP e implementar las actualizaciones de seguridad publicadas por el Proyecto PHP tan pronto como sea operacionalmente posible. La actualización constituye la medida de mitigación más efectiva para eliminar la condición vulnerable y reducir el riesgo de explotación.

Antes de desplegar las nuevas versiones en ambientes de producción, se recomienda realizar pruebas funcionales en entornos controlados que permitan verificar la compatibilidad de las aplicaciones institucionales, especialmente aquellas relacionadas con Historia Clínica

Electrónica, telemedicina, sistemas administrativos, RIS, PACS, LIS y plataformas de interoperabilidad clínica.

Mantener un inventario actualizado de aplicaciones desarrolladas sobre PHP

Las entidades deben disponer de un inventario completo de todas las aplicaciones desarrolladas sobre PHP, identificando la versión instalada, los componentes utilizados, las dependencias asociadas y los servicios externos con los cuales establecen comunicaciones mediante TLS.

Este inventario debe formar parte del proceso institucional de gestión de activos tecnológicos y permitir la priorización de actualizaciones cuando se publiquen nuevas vulnerabilidades que afecten componentes ampliamente utilizados dentro de la organización.

Fortalecer la gestión de vulnerabilidades

Las organizaciones deben incorporar esta vulnerabilidad dentro de sus procesos de gestión de vulnerabilidades, asegurando la identificación continua de componentes afectados, la evaluación del nivel de exposición y la implementación oportuna de medidas de remediación.

Se recomienda complementar los procesos de actualización con herramientas automáticas de análisis de vulnerabilidades, escaneo continuo de infraestructura, revisión periódica de boletines de seguridad del Proyecto PHP y seguimiento permanente de las alertas emitidas por fabricantes, CERT nacionales y organismos internacionales especializados en ciberseguridad.

Supervisar continuamente el comportamiento de las conexiones TLS

Los equipos de infraestructura y ciberseguridad deben fortalecer el monitoreo de los procesos relacionados con el establecimiento de conexiones TLS, incorporando mecanismos que permitan identificar comportamientos anómalos durante la negociación criptográfica.

Se recomienda supervisar registros generados por PHP, PHP-FPM, Apache HTTP Server, Nginx, balanceadores de carga, proxies inversos, sistemas operativos y plataformas SIEM, con el fin de detectar terminaciones inesperadas de procesos, errores repetitivos durante conexiones seguras, reinicios continuos de servicios o patrones que evidencien intentos de explotación de la vulnerabilidad.

La correlación de estos eventos permitirá reducir significativamente el tiempo requerido para identificar incidentes y ejecutar medidas de contención antes de que el impacto operacional afecte otros servicios institucionales.

Implementar mecanismos de alta disponibilidad y tolerancia a fallos

Las aplicaciones críticas utilizadas por el sector salud deben ejecutarse sobre arquitecturas que incorporen mecanismos de alta disponibilidad, balanceo de carga y recuperación automática de servicios.

La implementación de múltiples instancias de servidores PHP, balanceadores de carga, plataformas de orquestación, redundancia geográfica y mecanismos de failover contribuye a reducir el impacto operacional derivado de interrupciones inesperadas sobre componentes individuales de la infraestructura tecnológica.

Estas medidas resultan especialmente importantes para plataformas de Historia Clínica Electrónica, telemedicina, interoperabilidad clínica y servicios utilizados durante procesos asistenciales de alta criticidad.

Revisar las dependencias externas utilizadas por las aplicaciones

Las organizaciones deben identificar todos los servicios externos con los cuales interactúan las aplicaciones desarrolladas sobre PHP, incluyendo APIs REST, servicios SOAP, plataformas de autenticación, proveedores de identidad, servicios de correo electrónico, soluciones de almacenamiento en la nube y plataformas de interoperabilidad.

El conocimiento detallado de estas dependencias permitirá evaluar el impacto potencial que una interrupción de las conexiones TLS podría generar sobre los procesos institucionales y facilitará la implementación de mecanismos alternativos de comunicación cuando sea necesario.

Fortalecer el monitoreo mediante plataformas SIEM

Se recomienda incorporar eventos relacionados con conexiones TLS dentro de las plataformas institucionales de gestión de eventos e información de seguridad (SIEM), correlacionando registros provenientes de servidores web, sistemas operativos, dispositivos de seguridad perimetral, soluciones EDR/XDR y herramientas de monitoreo de infraestructura.

La construcción de reglas específicas de correlación permitirá identificar patrones asociados con fallos repetitivos durante el establecimiento de conexiones seguras, incrementando la capacidad institucional para detectar oportunamente intentos de explotación y responder de manera coordinada.

Fortalecer las capacidades de respuesta a incidentes

Los procedimientos institucionales de respuesta a incidentes deben incorporar escenarios específicos relacionados con vulnerabilidades que afecten componentes base ampliamente utilizados por aplicaciones empresariales.

Los equipos responsables de infraestructura, continuidad del negocio y ciberseguridad deben disponer de procedimientos documentados para identificar rápidamente aplicaciones vulnerables, aislar servicios afectados, implementar medidas temporales de contención, ejecutar procesos de recuperación y validar la correcta operación de las plataformas antes de restablecer completamente los servicios.

Realizar pruebas periódicas de continuidad del negocio

Las organizaciones deben desarrollar ejercicios periódicos orientados a validar la capacidad institucional para responder ante escenarios de indisponibilidad de aplicaciones críticas ocasionados por vulnerabilidades de software.

Estas pruebas deben contemplar la activación de planes de contingencia, recuperación de servicios, validación de respaldos, restablecimiento de aplicaciones críticas y evaluación de tiempos de recuperación (RTO) y puntos objetivos de recuperación (RPO), especialmente para plataformas que soportan procesos clínicos esenciales.

Implementar una estrategia de actualización continua de componentes tecnológicos

Las entidades del sector salud deben establecer una estrategia formal para la administración del ciclo de vida de los componentes tecnológicos utilizados por sus aplicaciones.

Esta estrategia debe contemplar la identificación permanente de nuevas versiones de software, la evaluación del impacto de vulnerabilidades recientemente divulgadas, la programación periódica de actualizaciones y la eliminación progresiva de componentes que hayan alcanzado el fin de su ciclo de soporte.

La actualización continua de componentes como PHP, bibliotecas criptográficas, servidores web y frameworks de desarrollo constituye uno de los controles más efectivos para reducir la superficie de ataque y fortalecer la resiliencia cibernética institucional.

Finalmente, el **CSIRT Salud** recomienda a todas las entidades del sector mantener una vigilancia permanente sobre la evolución de las vulnerabilidades que afectan componentes ampliamente utilizados dentro de las aplicaciones institucionales. La implementación temprana de actualizaciones de seguridad, el fortalecimiento de los procesos de gestión de vulnerabilidades, el monitoreo continuo de la infraestructura tecnológica y la adopción de arquitecturas resilientes contribuirán significativamente a reducir el impacto que este tipo de amenazas puede generar sobre la disponibilidad, continuidad e interoperabilidad de los servicios digitales que soportan la atención en salud.

Conclusiones

La vulnerabilidad **CVE-2026-12184** evidencia que incluso componentes ampliamente utilizados y considerados fundamentales para el funcionamiento de aplicaciones empresariales pueden convertirse en un vector de afectación para la continuidad operacional cuando presentan errores en el procesamiento de protocolos de comunicación seguros. Aunque el impacto técnico de esta vulnerabilidad se limita a la **disponibilidad** y no existen evidencias de ejecución remota de código, escalamiento de privilegios o divulgación directa de información, la interrupción de aplicaciones críticas representa un riesgo significativo para organizaciones cuya operación depende del intercambio permanente de información mediante conexiones protegidas por **Transport Layer Security (TLS)**.

En el sector salud, donde la transformación digital ha incrementado la dependencia de plataformas web para soportar procesos clínicos, administrativos y de interoperabilidad, la disponibilidad de los servicios constituye un elemento esencial para garantizar la continuidad de la atención. Aplicaciones como la **Historia Clínica Electrónica (HCE)**, los sistemas de información hospitalaria (HIS), las plataformas de laboratorio (LIS), los sistemas RIS y PACS, los servicios de telemedicina y las soluciones de interoperabilidad requieren mantener comunicaciones seguras y permanentes con múltiples servicios internos y externos. En este contexto, una condición de Denegación de Servicio que afecte dichas comunicaciones puede generar retrasos en la prestación del servicio, afectar procesos asistenciales y aumentar significativamente la carga operativa de los equipos responsables de la infraestructura tecnológica.

La publicación de **CVE-2026-12184** también pone de manifiesto la importancia de fortalecer los procesos institucionales de **gestión de vulnerabilidades, gestión de activos tecnológicos y administración del ciclo de vida del software**. La capacidad de identificar oportunamente los componentes afectados, evaluar su nivel de exposición y aplicar las actualizaciones de seguridad publicadas por los fabricantes constituye uno de los mecanismos más efectivos para reducir la superficie de ataque y limitar el impacto derivado de vulnerabilidades conocidas.

De igual manera, esta vulnerabilidad resalta la necesidad de implementar estrategias de **monitoreo continuo, observabilidad de aplicaciones y correlación de eventos de seguridad**, permitiendo identificar de forma temprana comportamientos anómalos asociados al

establecimiento de conexiones TLS, terminaciones inesperadas de procesos, errores repetitivos de comunicación o degradaciones progresivas del servicio. La integración de estos eventos dentro de plataformas SIEM y soluciones de detección y respuesta facilita una reacción más rápida frente a incidentes y contribuye a disminuir el tiempo medio de detección (MTTD) y el tiempo medio de recuperación (MTTR).

Las organizaciones del sector salud deben considerar que la explotación de vulnerabilidades orientadas a la disponibilidad puede generar consecuencias operacionales comparables a las producidas por otras categorías de amenazas, especialmente cuando afectan aplicaciones utilizadas durante la prestación de servicios asistenciales. La indisponibilidad temporal de plataformas críticas puede obligar a activar procedimientos de contingencia, utilizar procesos manuales, reprogramar actividades clínicas y destinar recursos adicionales para la recuperación de la operación, incrementando el riesgo operacional y afectando la eficiencia institucional.

Finalmente, el **CSIRT Salud** recomienda mantener una vigilancia permanente sobre los boletines de seguridad publicados por el **Proyecto PHP**, los fabricantes de software, los CERT nacionales e internacionales y las autoridades competentes en materia de ciberseguridad. La actualización continua de componentes tecnológicos, la aplicación de arquitecturas resilientes, la implementación de controles preventivos y el fortalecimiento de las capacidades institucionales de detección, respuesta y recuperación contribuirán significativamente a incrementar la resiliencia cibernética del sector salud y a reducir el impacto que vulnerabilidades como **CVE-2026-12184** pueden generar sobre la disponibilidad, continuidad y confiabilidad de los servicios digitales que soportan la atención de los pacientes.

Fuentes:

- <https://securityonline.info/php-remote-dos-cve-2026-12184/>
- <https://www.cve.org/CVERecord?id=CVE-2026-12184>
- <https://nvd.nist.gov/vuln/detail/CVE-2026-12184>
- <https://github.com/php/php-src/security/advisories/GHSA-mhmq-mmjq-2v39>
- <https://github.com/php/php-src/issues/21468>
- <https://github.com/php/php-src/commit/7782b8876bc0f61b0e8bcce262e22896e423b22e>
- <https://www.php.net/>

- <https://www.php.net/ChangeLog-8.php>
- <https://attack.mitre.org/>
- <https://cwe.mitre.org/>
- <https://owasp.org/www-project-web-security-testing-guide/>
- <https://owasp.org/www-project-top-ten/>
- <https://www.rfc-editor.org/rfc/rfc8446>
- <https://www.php.net/manual/en/book.openssl.php>

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) 316 893 1490 - 318 155 3570** o mediante el correo electrónico **csirtsalud@minsalud.gov.co**. Nuestro equipo está disponible para brindar el acompañamiento necesario.