CSIRT Salud

Boletín informativo

CSIRTSALUD-AL-20260604-51

TLP: CLEAR

Alerta ID:	051
Fecha del reporte:	04/06/2026
Entidad:	Todas las entidades del ecosistema digital
Título:	Vulnerabilidades en **Apache Tomcat**
Herramienta de detección	N/A
Activo involucrado:	Aplicaciones Java
Tipo de alerta:	Alerta
Nivel de riesgo:	Alto

Objetivo:

Informar a las organizaciones del sector salud en Colombia sobre la identificación de la vulnerabilidad crítica **CVE-2026-41293** en **Apache Tomcat (Ubuntu packaging)**, que afecta el manejo de encabezados HTTP/2 y puede permitir que aplicaciones web procesen datos malformados, comprometiendo la confidencialidad, integridad y disponibilidad de los sistemas.

El propósito de esta alerta es que las organizaciones del sector salud **valide si están utilizando versiones vulnerables de Tomcat**, tanto en infraestructura propia como en servicios en la nube o gestionados por terceros, revisando inventarios tecnológicos, servidores de aplicaciones web, portales clínicos y plataformas de integración de datos sensibles, con el fin de proteger la información crítica de pacientes y garantizar la continuidad de operaciones clave en el sector.

.

Descripción:

La vulnerabilidad **CVE-2026-41293** es una falla crítica en **Apache Tomcat (Ubuntu packaging)** que afecta el manejo de **encabezados HTTP/2**, permitiendo que aplicaciones web procesen datos malformados. Esta vulnerabilidad puede derivar en **comportamientos inesperados de las aplicaciones**, incluyendo posibles bypass de validaciones de seguridad, errores en la interpretación de datos o exposición de información sensible.

Afecta a múltiples versiones de Apache Tomcat, incluyendo:

- 9.0.0.M1 hasta 9.0.117
- 10.1.0.M1 hasta 10.1.54
- 11.0.0-M1 hasta 11.0.21

El fallo puede impactar **servidores web y aplicaciones críticas en entornos sanitarios**, como portales de pacientes, sistemas de historia clínica electrónica, bases de datos y servicios integrados en la nube.

Actualmente, se recomienda **actualizar a las versiones parcheadas** de Tomcat disponibles, ya que la explotación de esta vulnerabilidad puede ser remota y no requiere autenticación. Implementar medidas de mitigación temporales, como WAF o filtros de validación de solicitudes HTTP/2, es crucial para prevenir ataques mientras se aplica el parche oficial

Consecuencias de la explotación

La explotación de la vulnerabilidad **CVE-2026-41293** en Apache Tomcat puede tener varias consecuencias graves para las organizaciones del sector salud que utilizan aplicaciones web basadas en este servidor. Entre las principales se incluyen:

1. **Acceso no autorizado a aplicaciones críticas:** La vulnerabilidad permite que un atacante remoto envíe encabezados HTTP/2 malformados que puedan ser procesados incorrectamente, comprometiendo la integridad y disponibilidad de aplicaciones web críticas, como portales de pacientes, sistemas de historia clínica electrónica (HCE) y plataformas de integración de datos clínicos.
2. **Riesgo para la confidencialidad de los datos de los pacientes:** Si las aplicaciones utilizan encabezados HTTP/2 para decisiones de seguridad o permisos, un atacante podría acceder a información sensible, incluyendo datos médicos, historiales clínicos o información financiera de pacientes, vulnerando la privacidad y regulaciones de protección de datos.
3. **Interrupción de servicios y operaciones críticas:** La explotación puede provocar errores en la aplicación, caída de servicios web o mal funcionamiento de funcionalidades esenciales, afectando la atención de pacientes y la operación de sistemas administrativos y clínicos.
4. **Pérdida de confianza y reputación:** Un incidente derivado de esta vulnerabilidad podría afectar la reputación de la organización y disminuir la confianza de pacientes y socios, con potenciales sanciones regulatorias.
5. **Impacto económico:** Los costos pueden incluir la reparación de aplicaciones web, restauración de datos, mitigación de la vulnerabilidad y posibles multas regulatorias. También puede generar interrupciones operativas y pérdida de productividad.
6. **Posible acceso a otros sistemas conectados:** Dependiendo de la arquitectura, un atacante podría usar esta vulnerabilidad como punto inicial para explorar otras aplicaciones web o servicios internos, aumentando el riesgo de exposición de información sensible o compromiso adicional de sistemas críticos

Modo de explotación del ataque

La vulnerabilidad **CVE-2026-41293** en Apache Tomcat puede ser explotada de manera remota por un atacante sin necesidad de autenticación. La explotación se desarrolla de la siguiente forma:

Requisito inicial: acceso a la aplicación web

El atacante solo necesita poder enviar solicitudes HTTP/2 a un servidor Apache Tomcat vulnerable, lo cual puede realizarse a través de Internet o de una red interna accesible.

Explotación de la vulnerabilidad en encabezados HTTP/2

La falla reside en la **validación insuficiente de encabezados HTTP/2** antes de que sean procesados por la aplicación web. Un atacante puede enviar encabezados malformados o manipulados que provocan que la aplicación interprete incorrectamente los datos, generando potenciales rutas inseguras.

Impacto sobre la aplicación y la infraestructura

- **Manipulación de la lógica de la aplicación:** La aplicación puede procesar datos de forma inesperada, lo que puede afectar la seguridad de rutas internas, permisos o reglas de control.
- **Acceso a información sensible:** En aplicaciones web sanitarias, esta falla podría permitir la exposición de información de pacientes o datos financieros si los encabezados se usan para decisiones de seguridad.
- **Desestabilización del servicio:** Encabezados malformados pueden causar errores en la aplicación o interrumpir servicios críticos.

Acciones posteriores a la explotación

- **Reconocimiento de la infraestructura interna:** El atacante puede usar la falla para identificar rutas, servicios y componentes vulnerables dentro de la aplicación web.
- **Preparación para ataques adicionales:** La vulnerabilidad podría ser un punto de entrada para inyecciones, escalamiento de privilegios de aplicación o movimientos laterales hacia otros sistemas web conectados.
- **Impacto en servicios críticos:** Sistemas de gestión de pacientes, portales clínicos o servicios web internos podrían verse afectados, comprometiendo la confidencialidad, integridad y disponibilidad de la información.

Vulnerabilidades asociadas

- La explotación de CVE-2026-41293 se centra en el manejo incorrecto de encabezados HTTP/2 y puede derivar en varios problemas de seguridad en aplicaciones web que utilizan Apache Tomcat:
- **Validación insuficiente de encabezados HTTP/2:**

Descripción: Tomcat no valida correctamente los encabezados de solicitud HTTP/2 antes de exponerlos a la aplicación web, permitiendo que datos malformados sean procesados.

Impacto: Las aplicaciones pueden interpretar incorrectamente los valores de los encabezados, comprometiendo lógica de seguridad, acceso a recursos o flujo de control de la aplicación.

- **Exposición de servicios web a Internet sin filtros adicionales:**

Descripción: Servidores Tomcat expuestos sin WAF o validación adicional permiten que atacantes remotos envíen encabezados maliciosos.

Impacto: Puede dar acceso indirecto a funcionalidades sensibles o información confidencial, especialmente en aplicaciones críticas de salud.

- **Fallas en la gestión de sesiones y cookies de aplicación:**

Descripción: Aplicaciones que dependen de encabezados HTTP/2 para la generación de sesiones o autorización pueden ser vulnerables si no sanitizan adecuadamente los datos.

Impacto: Un atacante puede eludir mecanismos de autenticación de la aplicación o comprometer la integridad de las sesiones.

- **Dependencia de versiones no parcheadas de Tomcat:**

Descripción: Servidores con versiones anteriores a las corregidas (9.0.118+, 10.1.55+, 11.0.22+) permanecen vulnerables.

Impacto: Incluso si se aplica mitigación temporal, la exposición persiste hasta actualizar a la versión segura.

- **Potencial de escalamiento de ataques y movimiento lateral dentro de la aplicación web:**

Descripción: Encabezados malformados pueden permitir al atacante explorar rutas internas, parámetros sensibles o servicios conectados.

Impacto: Puede servir como base para explotación adicional dentro de la infraestructura de aplicaciones conectadas, afectando sistemas internos críticos o bases de datos de pacientes.

- **Relación con otras vulnerabilidades en entornos web**:

Fallas en la validación de input: Muchas vulnerabilidades críticas en aplicaciones web surgen de falta de saneamiento de datos de entrada, incluyendo encabezados HTTP, parámetros GET/POST y cookies.

- **Configuración inadecuada de WAF o filtros de seguridad**: La ausencia de inspección de tráfico HTTP/2 aumenta el riesgo de explotación de CVE-2026-41293.
- **Uso de versiones antiguas de Tomcat o librerías dependientes:** Servidores desactualizados o sin mantenimiento adecuado pueden amplificar el riesgo de explotación

Recomendaciones de detección y mitigación

1. Para detectar y mitigar eficazmente la amenaza representada por **CVE-2026-41293**, se recomienda que las entidades implementen medidas de seguridad avanzadas orientadas a la identificación de solicitudes malformadas HTTP/2 y la protección de aplicaciones web críticas:
2. **Mitigación temporal:** Implementar un WAF (Web Application Firewall) o filtros de validación para bloquear encabezados HTTP/2 malformados mientras se actualiza Apache Tomcat a la versión parcheada.
3. **Revisión de infraestructura:** Verificar que todos los servidores Tomcat ejecuten versiones parcheadas (9.0.118+, 10.1.55+, 11.0.22+). Auditar servidores expuestos a Internet o internos que utilicen HTTP/2.
4. **Monitoreo constante:** Activar alertas de seguridad en logs de Tomcat, aplicaciones web y proxies para identificar tráfico anómalo o solicitudes con encabezados HTTP/2 malformados.

5. **Control de accesos:** Revisar privilegios de cuentas que administren los servidores y aplicar el principio de mínimo privilegio para evitar escalamiento de explotación indirecta a otros sistemas.
6. **Relación con otras vulnerabilidades en entornos web:**
7. **Fallas en la validación de entradas:** Servidores que no validan adecuadamente encabezados, parámetros GET/POST o cookies pueden ser vulnerables a ataques similares.
8. **Configuraciones débiles de WAF o filtros de seguridad:** La ausencia de inspección de HTTP/2 incrementa la exposición.
9. **Uso de versiones antiguas de Tomcat:** Servidores que no reciben mantenimiento adecuado son más susceptibles a explotación de CVE-2026-41293 y otras vulnerabilidades de input validation.

Recomendaciones de prevención y mitigación:

Para mitigar los riesgos asociados con la vulnerabilidad **CVE-2026-41293**, es esencial actualizar inmediatamente Apache Tomcat a la versión parcheada y reforzar los controles de seguridad en aplicaciones web y servidores:

1. **Actualización inmediata de Tomcat:**
    - Instalar las versiones parcheadas: 9.0.118+, 10.1.55+ o 11.0.22+.
    - Asegurarse de que las implementaciones locales, en contenedores o en la nube estén actualizadas y configuradas para recibir actualizaciones automáticas.
2. **Filtrado de solicitudes HTTP/2:**
    - Implementar WAF o reglas de validación para bloquear encabezados HTTP/2 malformados.
    - Asegurarse de que el servidor web no procese datos de entrada sin validación.

3. **Fortalecer seguridad de aplicaciones web:**
    - Revisar y reforzar mecanismos de autenticación y autorización en las aplicaciones web que dependen de Tomcat.
    - Aplicar principios de mínimo privilegio en cuentas de aplicación y servicios.
4. **Políticas de firewall y control de red:**
    - Configurar firewalls de host y de perímetro para limitar accesos remotos solo a usuarios y sistemas autorizados.
    - Inspeccionar tráfico HTTP/2 para detectar anomalías o patrones sospechosos.
5. **Monitoreo de actividad de aplicaciones y servidores:**
    - Activar auditoría y alertas en Tomcat, proxies y WAF.
    - Monitorear logs de aplicaciones para detectar entradas HTTP/2 anómalas o patrones inusuales de acceso.
6. **Auditoría y verificación periódica:**
    - Revisar periódicamente la integridad de la configuración del servidor y las versiones de Tomcat.
    - Evaluar y auditar la seguridad de aplicaciones web y dependencias críticas.
7. **Capacitación del personal:**
    - Entrenar a administradores de servidores y personal técnico sobre prácticas de seguridad en aplicaciones web y manejo seguro de HTTP/2.
    - Promover concienciación sobre la explotación de encabezados malformados y mitigación de vulnerabilidades en servidores de aplicaciones.
8. **Implementación de políticas de seguridad estrictas:**
    - Establecer procedimientos claros para gestión de vulnerabilidades, aplicación de parches y monitoreo de seguridad.

- Incluir controles de revisión antes de exponer servidores a Internet o integrarlos a servicios en la nube.

Recomendaciones de respuesta ante compromiso:

- Si se sospecha que un servidor o aplicación ha sido comprometido debido a la explotación de **CVE-2026-41293**, es esencial actuar de inmediato para contener el incidente, mitigar daños y restaurar la seguridad:
- **Aislamiento del sistema afectado:**
- Desconectar el servidor Tomcat comprometido de la red para evitar explotación adicional o movimiento lateral.
- Si es posible, mantener logs y sesiones activas para análisis forense; en servidores críticos, deshabilitar interfaces de red temporalmente.
- **Análisis y confirmación del compromiso:**
- Revisar exhaustivamente los registros de Tomcat, logs de aplicación web, proxies y firewall para identificar solicitudes HTTP/2 malformadas o patrones anómalos.
- Detectar accesos no autorizados o modificaciones de archivos de configuración críticos.
- **Herramientas de análisis forense:**
- Utilizar herramientas de inspección de logs y auditoría (por ejemplo, WAF logs, SIEM, o herramientas de análisis de tráfico HTTP/2) para identificar vectores de explotación.
- **Contención del ataque:**
- Revocar o limitar temporalmente cuentas de administrador de aplicaciones web o servidores que pudieran haber sido comprometidas.
- Restablecer contraseñas y habilitar autenticación multifactor (MFA) para todos los accesos administrativos.
- Bloquear o filtrar temporalmente solicitudes HTTP/2 sospechosas mediante WAF o reglas de firewall mientras se aplica la actualización de Tomcat.

- **Erradicación y recuperación:**
- Actualizar inmediatamente Apache Tomcat a la versión parcheada correspondiente (9.0.118+, 10.1.55+, 11.0.22+).
- Verificar integridad de configuraciones críticas y restaurar cualquier archivo o parámetro modificado por el atacante.
- Revisar las aplicaciones conectadas al servidor comprometido para detectar posibles impactos o vulnerabilidades derivadas.
- **Auditoría post-incidente:**
- Realizar análisis completo de logs y tráfico para asegurar que no haya persistencia de la explotación.
- Documentar el incidente, las acciones realizadas y las medidas preventivas implementadas.
- Fortalecer políticas de seguridad, monitoreo y validación de entradas HTTP/2 para prevenir futuras explotaciones.

Erradicación de la Amenaza:

- **Actualización del servidor Tomcat:**
  - Una vez aislado el servidor y confirmada la explotación, actualizar Apache Tomcat a la versión parcheada correspondiente: 9.0.118+, 10.1.55+ o 11.0.22+.
  - Verificar que la actualización se haya aplicado correctamente y que el servicio web funcione con normalidad.
- **Búsqueda y eliminación de posibles backdoors:**
  - Revisar si se han instalado scripts maliciosos, configuraciones alteradas o módulos que permitan persistencia del ataque.
  - Utilizar herramientas de auditoría de aplicaciones y logs (WAF, SIEM) para detectar tráfico sospechoso y entradas anómalas.

- Eliminar cualquier proceso, archivo o configuración no autorizada detectada durante el análisis.

Restauración del Sistema:

- **Restauración desde copias de seguridad confiables:**
  - Si existen backups previos al incidente, restaurar el sistema y aplicaciones web a su estado funcional anterior.
  - Verificar la integridad de las copias de seguridad para asegurar que no contengan datos o configuraciones comprometidas.
- **Reinstalación de sistemas críticos:**
  - Si no se puede confiar plenamente en la integridad del servidor, considerar reinstalar Apache Tomcat y las aplicaciones afectadas, aplicando parches de seguridad antes de ponerlas en producción.

Comunicación y Notificación:

- **Notificación interna:** Informar al equipo de seguridad informática, administradores de sistemas y dirección sobre el compromiso para coordinar la respuesta y evaluación del impacto.
- **Notificación a terceros:** Si se ha expuesto información sensible de pacientes o datos críticos de la aplicación, notificar a autoridades regulatorias pertinentes, proveedores de servicios en la nube o proveedores de seguridad que soporten la infraestructura.

Prevención a Largo Plazo:

- **Auditorías periódicas de seguridad:** Realizar revisiones exhaustivas del servidor y aplicaciones web para detectar vulnerabilidades residuales y confirmar la eficacia de los parches aplicados.
- **Monitoreo continuo:** Supervisar logs, solicitudes HTTP/2 y alertas de seguridad para identificar cualquier actividad anómala después de la remediación.
- **Mejora de políticas de seguridad:** Reforzar la gestión de parches, la validación de entradas y la configuración de seguridad de Tomcat, incluyendo WAF y controles de autenticación, para prevenir futuros incidentes.
- **Gestión de vulnerabilidades:** Implementar un proceso sistemático de identificación y corrección rápida de fallos de seguridad en aplicaciones web y servidores de producción.

Conclusiones

La vulnerabilidad **CVE-2026-41293** en Apache Tomcat representa una amenaza crítica debido a que permite a atacantes remotos enviar encabezados HTTP/2 malformados, lo que puede comprometer la integridad y disponibilidad de aplicaciones web y servicios críticos del sector salud.

Las organizaciones que utilicen Tomcat para portales de pacientes, sistemas de historia clínica electrónica (HCE) o aplicaciones web de gestión sanitaria corren el riesgo de:

- Exposición de datos sensibles de pacientes.
- Interrupción de servicios críticos y aplicaciones web internas.
- Posibles movimientos laterales hacia otros sistemas conectados si la explotación inicial no se detecta.

La **aplicación inmediata de la actualización de Tomcat** es la medida más efectiva para mitigar el riesgo. Mientras tanto, implementar filtros de HTTP/2, auditorías de logs y supervisión activa de tráfico web son pasos esenciales para contener la amenaza.

Después de la remediación, las organizaciones deben:

- Realizar auditorías periódicas de seguridad en los servidores y aplicaciones web.
- Fortalecer políticas de gestión de parches y controles de seguridad de aplicaciones.
- Capacitar al personal técnico en la identificación de patrones de explotación y en buenas prácticas de ciberseguridad.
- Aplicar autenticación multifactor y principios de mínimo privilegio para reducir el riesgo de futuras explotaciones.

Fuentes:

1. **Apache Tomcat Security Advisory:** Boletín oficial con detalles de la vulnerabilidad CVE-2026-41293 y versiones parcheadas.
   Enlace: https://advisories.gitlab.com/maven/org.apache.tomcat/tomcat/CVE-2026-41293
   Descripción: Información técnica detallada sobre la falla de validación de encabezados HTTP/2 y las versiones afectadas.
2. **Ubuntu Security Notice:** Información oficial de paquetes de Tomcat vulnerables y actualización en distribuciones Ubuntu.
   Enlace: https://ubuntu.com/security/CVE-2026-41293
   Descripción: Detalle de la vulnerabilidad aplicada al empaquetado de Tomcat en Ubuntu y las acciones de mitigación.
3. **CVE Database – NVD / MITRE:** Registro oficial del CVE con métricas de severidad y vectores de ataque.

Enlace: https://nvd.nist.gov/vuln/detail/CVE-2026-41293
Descripción: Clasificación CVSS, descripción técnica y referencias a fuentes oficiales.

4. **Threat Intelligence / Exploit Reports:** Análisis de explotación remota de encabezados HTTP/2 malformados y riesgos para aplicaciones web críticas.
   Enlace: https://www.threatclaw.ai/cve/CVE-2026-41293
   Descripción: Información de vectores de ataque y mitigación en entornos de producción.
5. **MITRE ATT&CK Framework for Enterprise:** Referencias a tácticas y técnicas aplicables a la explotación de validación insuficiente de entrada en aplicaciones web.
   Enlace: https://attack.mitre.org/
   Descripción: Mapeo de técnicas de movimiento lateral, evasión y explotación de aplicaciones web.

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.