Incidente ID:	0024
Fecha del reporte:	13/01/2026
Entidad:	Todas las Entidades del Ecosistema Digital
Título:	Vulnerabilidad en Angular
Herramienta de detección	N/A
Activo involucrado:	Angular
Tipo de incidente:	Boletín informativo
Nivel de riesgo:	Alto

Objetivo:

Informar a las entidades del Ecosistema Digital sobre una vulnerabilidad cross-site scripting (XSS), la cual afecta el compilador de plantillas de Angular, esta vulnerabilidad fue calificada con una puntuación CVSS:8.5 la cual es catalogada como crítica.

Descripción:

Se ha identificado una vulnerabilidad de Cross-Site Scripting (XSS) de severidad alta en el Compilador de Plantillas de Angular (*Angular Template Compiler*). Esta falla afecta a los paquetes @angular/compiler y @angular/core.

La vulnerabilidad reside en el mecanismo de sanitización de Angular, específicamente en cómo gestiona los atributos de los elementos SVG. El parche proporcionado en la solicitud de incorporación de cambios n.° 66318 muestra claramente la corrección en la getUrlSanitizerfunción ubicada en packages/core/src/sanitization/sanitization.ts. Antes del parche, esta función no reconocía href ni xlink:href en una etiqueta SVG <script> como un contexto que requería una sanitización estricta de la URL del recurso. El parche corrige esto añadiendo lógica para identificar esta combinación específica y aplicar el sanitizado adecuado

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

(ɵɵsanitizeResourceUrl). El cambio en packages/compiler/src/schema/dom_security_schema .ts es una parte relacionada con la corrección, que actualiza el esquema que utiliza el compilador, pero getUrlSanitizer es la función que se invocaría en tiempo de ejecución para tomar la decisión de sanitización. Por lo tanto, getUrlSanitizer es la función vulnerable clave que, al ser explotada, formaría parte del flujo de ejecución que conduce al XSS.

Productos afectados:

La vulnerabilidad afecta a todas las versiones de Angular anteriores a los parches lanzados en enero de 2026. Específicamente**:**

Paquete Angular	Versiones Vulnerables
@angular/compiler, @angular/core 21.x	Versiones anteriores a 21.0.7 y 21.1.0-rc.0
@angular/compiler, @angular/core 20.x	Versiones anteriores a 20.3.16
@angular/compiler, @angular/core 19.x	Versiones anteriores a 19.2.18
Versiones antiguas	Versiones anteriores sin soporte oficial también son vulnerables

Indicadores de compromiso

Dado que es una vulnerabilidad del lado del cliente (XSS), los IoCs tradicionales de red pueden ser limitados, pero se pueden buscar las siguientes firmas:

- Logs de WAF / Servidor Web: Búsqueda de patrones en peticiones HTTP (GET/POST) que contengan cadenas codificadas como <svg>, <script>, xlink:href combinados con esquemas data:text/javascript o javascript:.

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

- Auditoría de Base de Datos (Stored XSS): Si la aplicación permite guardar entradas de usuario que luego se renderizan, buscar en la base de datos cadenas que contengan:
  - <script [attr.href]
  - <script [attr.xlink:href]

- Comportamiento Anómalo: Reportes de usuarios sobre ventanas emergentes inesperadas, redirecciones no autorizadas o acciones realizadas en su nombre sin consentimiento.

Modo de explotación y cadena de infección

Para que dicha vulnerabilidad pueda ser explotada se tiene que cumplir las siguientes condiciones o parámetro:

- La aplicación víctima debe utilizar explícitamente <script>elementos SVG dentro de sus plantillas.
- La aplicación debe utilizar la vinculación de propiedades o atributos (interpolación) para los href atributos xlink:href de esos scripts SVG.
- Los datos vinculados a estos atributos deben derivarse de una fuente no confiable (por ejemplo, parámetros de URL, entradas de base de datos enviadas por el usuario o respuestas de API no desinfectadas).

Después de que se hallan cumplido las anteriores condiciones el atacante puede efectuar el ataque de la siguiente forma.

Un atacante puede explotar esto si la aplicación Angular realiza un *binding* (enlace de datos) dinámico a los atributos href o xlink:href de una etiqueta script dentro de un SVG.

Escenario de Código Vulnerable:

HTML
<svg>

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

```
  <script [attr.href]="userUrl"></script>
</svg>
```

Si la variable userUrl es controlada por el usuario, el atacante puede inyectar: data:text/javascript,alert('XSS Exploit Executed')

Al renderizarse, el navegador ejecutará el código JavaScript malicioso en el contexto de la sesión de la víctima, eludiendo el *Same-Origin Policy* (SOP) para acciones locales.

Técnica de ataque (Mitre ATT$CK)

Esta vulnerabilidad se alinea con las siguientes técnicas del marco MITRE ATT&CK:

- T1059.007 (Command and Scripting Interpreter: JavaScript): Ejecución de scripts maliciosos en el navegador de la víctima.
- T1189 (Drive-by Compromise): Si la inyección es persistente, los usuarios que visiten la página afectada serán comprometidos automáticamente.
- T1552 (Unsecured Credentials): Uso del XSS para robar tokens de sesión (cookies, localStorage).

Recomendaciones de mitigación:

La única solución completa es actualizar los paquetes de Angular a las versiones parcheadas liberadas, las cuales se pueden consultar en el siguiente enlace (https://angular.dev/reference/releases#actively-supported-versions).

- Si usa v21: Actualizar a v21.0.7 o superior.
- Si usa v20: Actualizar a v20.3.16 o superior.
- Si usa v19: Actualizar a v19.2.18 o superior.

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

Ejecute el siguiente comando en su proyecto:

Bash

ng update @angular/core @angular/cli

Mitigaciones temporales (En caso de no poder aplicar el parche inmediatamente)

- Evite enlazar dinámicamente ([attr.href]/[attr.xlink:href]) en SVG <script>. Refactorice para no depender de scripts SVG externos o elimine dichos elementos de las plantillas.
- Validación/allowlist estricta de URLs para cualquier atributo susceptible de cargar recursos, aplicada del lado servidor o antes del binding (solo dominios y rutas explícitamente permitidos).
- Defensas generales anti-XSS: encoding por contexto, CSP (Content Security Policy) que bloquee data: y scripts externos no autorizados, y auditorías con OWASP ZAP/Burp. (Buenas prácticas contra XSS).

Fuentes:

- https://cybersecuritynews.com/angular-vulnerability/
- https://angular.dev/reference/releases#actively-supported-versions
- https://www.cvedetails.com/cve/CVE-2026-22610/
- https://www.miggo.io/vulnerability-database/cve/CVE-2026-22610
- https://www.resolvedsecurity.com/vulnerability-catalog/CVE-2026-22610
- https://nvd.nist.gov/vuln/detail/CVE-2026-22610

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 8931490 - 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