Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

# INVESTIGADORES ENCUENTRAN UNA CADENA DE EXPLOITS EN SITECORE QUE COMBINA EL ENVENENAMIENTO DE CACHÉ CON RCE

*29/ 08 / 2025*

# CONTENIDO

# INTRODUCCIÓN

Investigadores de watchTowr Labs han revelado tres nuevas fallas críticas en la plataforma Sitecore Experience Platform (XP). Al ser encadenadas, estas vulnerabilidades permiten la ejecución remota de código (RCE) y el control total de la aplicación.

# INVESTIGADORES ENCUENTRAN UNA CADENA DE EXPLOITS EN SITECORE QUE COMBINA EL ENVENENAMIENTO DE CACHÉ CON RCE

A continuación, se encuentra en cuadro de identificación de la amenaza.

| | |
|---|---|
| **ID de alerta:** | DSOC-CERT_2025_08_29_2 |
| **Clasificación de alerta:** | Noticia |
| **Tipo de Impacto:** | Alta |
| **TLP (Clasificación de información):** | **CLEAR** |
| **Fecha de publicación:** | 29/08/2025 |
| **Es día cero (0 day):** | No |

# RESUMEN

Investigadores de watchTowr Labs han revelado tres nuevas fallas críticas en la plataforma Sitecore Experience Platform (XP). Al ser encadenadas, estas vulnerabilidades permiten la ejecución remota de código (RCE) y el control total de la aplicación.

**vulnerabilidades identificadas**

- CVE-2025-53693: Envenenamiento de caché HTML a través de un mecanismo inseguro de reflexión.
- CVE-2025-53691: Ejecución remota de código por deserialización insegura de objetos.
- CVE-2025-53694: Exposición de información a través de la API ItemService.

**¿Cómo funciona la cadena de ataque?**

1. Exfiltración de información: El atacante explota el CVE-2025-53694 para acceder a la API ItemService y obtener claves internas de caché, que deben ser inaccesibles.
2. Inyección de código: Con esa información, el atacante inyecta código malicioso en HTML usando el CVE-2025-53693, manipulando así la caché reflejada.
3. Ejecución remota de código: Finalmente, con el CVE-2025-53691, el contenido inyectado se deserializa de forma insegura (generalmente a través de BinaryFormatter en .NET), lo que permite ejecutar código arbitrario en el servidor.

**Un historial preocupante**

Esta no es la primera vez que Sitecore XP enfrenta vulnerabilidades críticas. En meses recientes, otros fallos ya habían sido descubiertos:

- CVE-2025-34509: Credenciales codificadas (ServicesAPI / “b”).
- CVE-2025-34510: Vulnerabilidad “Zip Slip” en cargas de ZIP.
- CVE-2025-34511: Carga de archivos no restringida en el módulo PowerShell.

Los expertos advierten que incluso los sistemas actualizados podrían seguir siendo vulnerables si no aplican todos los parches acumulativos y corrigen las configuraciones inseguras.

**Impacto y riesgo real**

- Blanco atractivo: Sitecore XP es un CMS muy utilizado en los sectores de gobierno, salud, finanzas y comercio minorista, lo que lo convierte en un objetivo de alto valor.
- Exposición frecuente: Muchas instancias de Sitecore están directamente conectadas a Internet, lo que aumenta la superficie de ataque.
- Potencial de ransomware: Una RCE encadenada podría usarse para desplegar ransomware o puertas traseras persistentes en servidores corporativos.
- Impacto en la cadena de suministro: Al ser un CMS, un compromiso podría afectar a sitios web de alto tráfico, campañas de marketing digital y datos de clientes.

## RECOMENDACIONES

- Instale la actualización SC2025-003, que corrige estos errores en Sitecore XP 9.0 a 10.4.
- Revise los accesos a la API ItemService y otros servicios que podrían estar abiertos al público.
- Active la autenticación multifactor (MFA) y limite el acceso a la administración de Sitecore solo desde redes internas o una VPN.
- Implementa la detección de intentos de fuerza bruta, patrones inusuales en el caché o la ejecución de procesos no habituales.

## NOTICIA COMPLETA

https://devel.group/blog/investigadores-hallan-una-cadena-de-exploits-en-sitecore-que-combina-el-envenenamiento-de-cache-con-rce/

# CONTACTOS DE SOPORTE


**Correo electrónico:** cti@develsecurity.com

**Teléfonos directos:**

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

**Sitio Web:** https://devel.group