Nro. Alerta:	AL-2026-037	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	21-jul-2026	Campaña de Defacement en Portales Institucionales Basados en Joomla en Ecuador	Pág.: **1** of **5**

I. DATOS GENERALES:

Clase de alerta: Ciberamenaza
Tipo de Incidente: Defacement Web
Nivel de riesgo: Alta

II. ALERTA

Figura 1.- Campaña de Defacement en Portales Institucionales Basados en Joomla en Ecuador - Figura referencial

Se ha detectado una campaña masiva de Defacement (desfiguración de sitios web) que explota las vulnerabilidades CVE-2026-48907, CVE-2026-48908 y CVE-2026-49049 presentes en el sistema de gestión de contenidos (CMS) de Joomla!. La explotación encadenada de estas vulnerabilidades permitiría a un atacante no autenticado crear cuentas con privilegios de editor, cargar archivos arbitrarios y ejecutar código de forma remota (RCE). Durante actividades de monitoreo de fuentes abiertas (OSINT), se identificó una campaña activa que aprovecha estas vulnerabilidades y que está dirigida contra diversos portales institucionales de Ecuador.

III. INTRODUCCIÓN

El Defacement es un tipo de ataque informático en el que un atacante modifica de manera no autorizada el contenido o la apariencia de un sitio web legítimo, alterando

sus páginas para mostrar mensajes, imágenes, propaganda, consignas o reivindicaciones ajenas a la organización propietaria. Los atacantes incorporan una firma o alias (*tag*) con el objetivo de atribuirse la intrusión y evidenciar que lograron comprometer el sitio web.

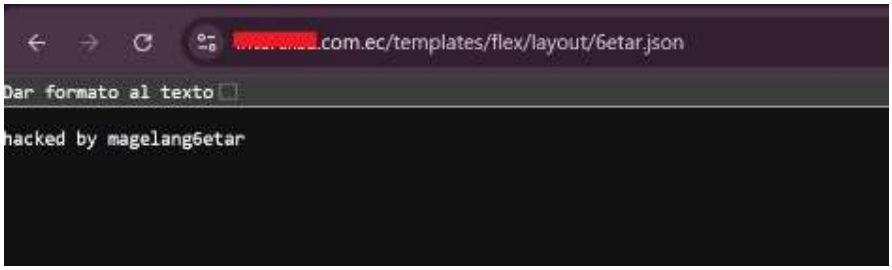

Figura 2-. Defacement en un sitio web de Ecuador con firma del atacante.

Joomla!, es un Sistema de Gestión de Contenidos (CMS) gratuito y de código abierto que permite crear, organizar y administrar sitios web a través de una interfaz gráfica, facilitando la gestión de contenidos sin requerir conocimientos avanzados de programación.

Figura 3. - Sitio Web basado en Joomla!.

Los Defacement estarían asociados con la explotación de tres vulnerabilidades críticas identificadas en extensiones ampliamente utilizadas del CMS Joomla!, correspondientes a: Joomla Content Editor (JCE) (CVE-2026-48907), SP Page Builder (CVE-2026-48908) y Helix3 (CVE-2026-49049).

La vulnerabilidad CVE-2026-48907 permite a un atacante crear un nuevo perfil de editor falso a través de **JCE** sin necesidad de autenticación, lo que a su vez le permite subir y ejecutar archivos PHP arbitrarios en el servidor web. Los investigadores concluyen que esta vulnerabilidad ha sido explotada para desplegar webshells en cientos de sitios web comprometidos e inclusive en el mes de junio se publicó en GitHub un exploit público de prueba de concepto (PoC).

La vulnerabilidad CVE-2026-48908 afecta **SP Page Builde**r, una extensión utilizada para la creación y gestión visual de páginas web en Joomla!. La falla permite que un atacante no autenticado cargue archivos arbitrarios en el servidor, lo que podría derivar en la ejecución de código PHP no autorizado y el compromiso del sistema afectado. De acuerdo con los reportes de seguridad disponibles, la vulnerabilidad está siendo explotada activamente en ataques reales.

La vulnerabilidad CVE-2026-49049, afecta al framework **Helix3**, que es utilizado en plantillas de Joomla!. La falla expone un handler AJAX que podría ser accedido por atacantes no autenticados para eliminar archivos arbitrarios, escribir archivos JSON y modificar parámetros de templates.

En Ecuador se ha detectado una campaña activa de Defacement dirigida contra diversas instituciones públicas y privadas que utilizan el CMS Joomla!. El análisis de los sitios web comprometidos permitió identificar mensajes de reivindicación y firmas de los atacantes **TRENGGALEK6ETAR**, **Antonkill** y **Simsimi**, observados de forma recurrente en múltiples páginas afectadas.

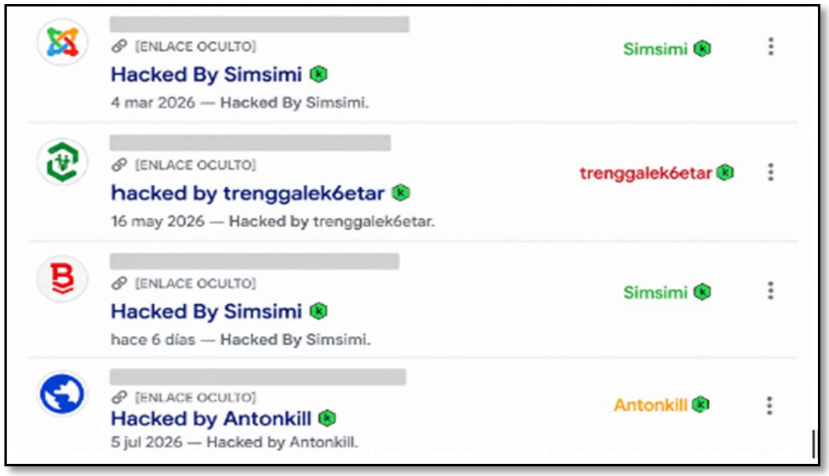

Figura 4.- Identificación de sitios web en Ecuador afectados por Defacement mediante búsquedas avanzadas con Google Dorks.

IV. VECTOR DE ATAQUE

La vulnerabilidad **CVE-2026-48907** tiene un vector de ataque tipo RED, CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/V con nivel de severidad 10 CRITICA.

La vulnerabilidad **CVE-2026-48908** tiene un vector de ataque tipo RED, CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H con nivel de severidad 9.8 CRITICA.

La vulnerabilidad **CVE-2026-49049** tiene un vector de ataque tipo RED, CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N con nivel de severidad 7.5 CRITICA.

V. IMPACTO

Producto	Evidencia
Joomla Content Editor (JCE)	versiones anteriores a 2.9.99.5
SP Page Builder	versiones anteriores a 6.6.2
Helix3	versiones 1.0 a 3.1.1 inclusive

Tabla 1.- Extensiones Joomla! que presentan vulnerabilidades.

VI. INDICADORES DE COMPROMISO

Atacantes	Firmas en Defacement
TRENGGALEK6ETAR	Pantalla "HACKED BY TRENGGALEK6ETAR"
Antonkill	Pantalla "HACKED BY Antonkill"
Simsimi	Pantalla "HACKED BY Simsimi"

Tabla 2. - Firmas de atacantes encontrados en las campanas defacement en Ecuador.

VII. RECOMENDACIONES:

- Actualizar Joomla Content Editor (JCE) a la versión 2.9.99.5 o posterior. En caso de no poder actualizar de forma inmediata por incompatibilidades con la versión de Joomla o PHP.
- Actualizar SP Page Builder a la versión 6.6.2 o posterior. Luego de la actualización, se deberá verificar que los archivos del componente hayan sido reemplazados correctamente y que no permanezcan archivos vulnerables o modificados dentro de las rutas del componente.

- Actualizar Helix3 a la versión más reciente disponible publicada por el proveedor. En particular, se deberá verificar la actualización de los plugins System - Helix3 Framework y Helix3 - Ajax.
- Configurar monitoreo de integridad de archivos.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

CERT PARAGUAY. (2026). *Vulnerabilidades en productos Joomla.* https://www.cert.gov.py/vulnerabilidades-en-productos-joomla-2/

CERTUY – CENTRO NACIONAL DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA. (2026). *Múltiples vulnerabilidades en componentes y extensiones de Joomla.* https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/comunicacion/noticias/multiples-vulnerabilidades-componentes-extensiones-joomla

SC MEDIA. (2026). *Max-severity Joomla content editor extension flaw targeted in automated attacks.* https://www.scworld.com/news/max-severity-joomla-content-editor-extension-flaw-targeted-in-automated-attacks

CENTRE FOR CYBERSECURITY BELGIUM (CCB). (2026). *Warning: Massive Content Management Software (CMS) defacement campaign observed.* https://ccb.belgium.be/advisories/warning-massive-content-management-software-cms-defacement-campaign-observed

HAND, W. (2026). *Ciberseguridad – Incident Response – Joomla* [Publicación de LinkedIn]. https://www.linkedin.com/posts/william-hand-a3203b396_ciberseguridad-incidentresponse-joomla-ugcPost-7479219759016873984-rW7O/