Boletín informativo
Vulnerabilidad en plugin Modular DS Connector

CSIRTSALUD-AV-20260115-25 **TLP: CLEAR**

Incidente ID:	0025
Fecha del reporte:	15/01/2026
Entidad:	Todas las Entidades del Ecosistema Digital
Título:	Vulnerabilidad plugin Modular DS Connector
Herramienta de detección	N/A
Activo involucrado:	WordPress
Tipo de incidente:	Boletín informativo
Nivel de riesgo:	Alto

Objetivo:

Informar a las entidades del Ecosistema Digital sobre la vulnerabilidad de nivel crítica identificada como CVE-2026-23550 (puntuación CVSS: 10.0), se ha descrito como un caso de escalada de privilegios no autenticado que afecta a todas las versiones del complemento Modular DS de WordPress anteriores a la 2.5.1. Esta vulnerabilidad se encuentra siendo explotada activamente.

Descripción:

Se ha identificado una vulnerabilidad de máxima severidad en el plugin Modular DS para WordPress. Modular DS, desarrollado por modulards.com, permite la gestión remota de múltiples sitios de WordPress, incluida la supervisión, las actualizaciones y las copias de seguridad.

El fallo reside en el mecanismo de enrutamiento de la API del plugin, específicamente en cómo valida las solicitudes entrantes. Los atacantes pueden activar el modo de "solicitud directa" usando origin=mo y cualquier tipo de parámetro, evadiendo el middleware de autenticación si el sitio está conectado a servicios modulares.

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

Esto expone rutas protegidas como /login/{modular_request}, donde AuthController inicia sesión automáticamente como usuario administrador mediante getAdminUser() si no se especifica ningún ID de usuario. Ninguna firma, secreto ni verificación de IP valida las solicitudes, lo que conlleva a una vulneración total mediante acciones como el borrado de caché, las copias de seguridad o la instalación de plugins.

En la versión 2.5.1, la ruta se comparaba primero con la URL controlada por el atacante. Por lo tanto, si un atacante llamaba a */api/modular-connector/login/anything?* ..., el enrutador resolvería automáticamente la ruta *login/{modular_request}* y la pasaría al filtro. Luego, en [nombre del host RouteServiceProvider::bindOldRoutes()], si no se reconocía el tipo (p. ej., foo), el código no recurriría a ninguna ruta alternativa y simplemente devolvería la ruta original (*/login/* ...).

Productos afectados:

La vulnerabilidad afecta exclusivamente al siguiente componente:

- Producto: Plugin Modular DS (anteriormente conocido como Modular Connector).
- Versiones Vulnerables: Todas las versiones anteriores e incluyendo la 2.5.1.
- Plataforma: WordPress (CMS).

Indicadores de compromiso

Los equipos de seguridad deben monitorear los registros de acceso (access logs) del servidor web y del WAF en busca de los siguientes patrones:

- Tráfico de Red Sospechoso: Peticiones HTTP dirigidas a la API del plugin que contengan el parámetro origin=mo.

Ejemplo *de Log:* GET /wp-json/modular-connector/v1/... ?origin=mo&type=...

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

- Accesos a Rutas Críticas: Intentos de acceso inusuales a las siguientes rutas sin una sesión previa válida:

    - /login/ (dentro del contexto de la API Modular)
    - /server-information/
    - /manager/
    - /backup/

Se ha identificado ataques originados desde las siguientes direcciones IP:

- 45.11.89[.]19
- 162.158.123[.]41
- 172.70.176[.]95
- 172.70.176[.]52

Modo de explotación y cadena de infección

La vulnerabilidad se encuentra en la lógica que maneja las "solicitudes directas" dentro del prefijo de ruta /api/modular-connector/.

Los vectores de ataque confirmados incluyen:

- AV:N – Acceso remoto sobre red.
- PR:N – No requiere privilegios previos.
- UI:N – No requiere interacción del usuario.
- AC:L – Baja complejidad del ataque.
- S:C – Cambio de alcance (el atacante puede ejecutar acciones como usuario administrador).

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

El plugin está diseñado para permitir ciertas solicitudes internas si contienen parámetros específicos. Se descubrió que al suministrar el parámetro origin con el valor mo y un parámetro type con cualquier valor arbitrario, el sistema "confía" ciegamente en la solicitud.

Al enviar una petición HTTP manipulada (ej. origin=mo&type=1), el middleware de autenticación asume que la petición es legítima y proviene de una fuente confiable, saltándose la verificación de tokens criptográficos o credenciales. Esto expone rutas críticas como /login/{modular_request}, permitiendo al atacante iniciar sesión automáticamente como el primer usuario administrador disponible en la base de datos.

El uso de esta vulnerabilidad suele alinearse con las siguientes tácticas y técnicas:

- TA0001 – Initial Access: Explotación de servicio público accesible.
- T1190 – Exploit Public-Facing Application: Explotar una vulnerabilidad remota sin autenticación.
- TA0004 – Privilege Escalation: Obtener privilegios administrativos dentro del CMS.
- T1068 – Privilege Escalation: Aprovechar permisos incorrectos.

Recomendaciones de mitigación:

Actualizar inmediatamente el plugin Modular DS a la versión 2.5.2 o superior. Esta versión introduce parches que validan correctamente el origen de las solicitudes y eliminan el bypass de autenticación, para realizar la actualización se puede realizar de las siguientes formas:

Desde Modular DS:

- Comprobar si hay actualizaciones disponibles desde el panel de Modular DS.
- Si la actualización no aparece, realizar clic en el botón “Recargar” del actualizador.
- Algunos sitios pueden tardar unos minutos en detectar la actualización. Las actualizaciones se están forzando progresivamente en todos los sitios.

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

Desde el panel de admin de WordPress:

- Ir a Plugins → Plugins instalados
- Buscar la notificación de actualización de Modular Connector (si usa white label, buscar el nombre personalizado que se haya configurado)
- Dar clic en “Actualizar”

Via WP-CLI:

wp plugin update modular-connector

Post-Incidente:

- Revisar todos los usuarios con rol de "Administrador" y eliminar cualquier cuenta no reconocida.
- Forzar un restablecimiento de contraseñas para todos los administradores.
- Escanear el sitio en busca de archivos modificados o nuevos plugins instalados desde la fecha del 13 de enero de 2026 (fecha en que se detectaron los primeros ataques masivos).

Fuentes:

- https://help.modulards.com/en/article/modular-ds-security-release-modular-connector-252-dm3mv0/
- https://patchstack.com/articles/critical-privilege-escalation-vulnerability-in-modular-ds-plugin-affecting-40k-sites-exploited-in-the-wild/
- https://app.opencve.io/cve/CVE-2026-23550
- https://thehackernews.com/2026/01/critical-wordpress-modular-ds-plugin.html
- https://cybersecuritynews.com/wordpress-plugin-vulnerability-admin-access/

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

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