Incidente ID:	0010
Fecha del reporte:	29/10/2025
Entidad:	Todas las Entidades del Ecosistema Digital
Título:	Explotación masiva de vulnerabilidad en plugins de WordPress
Herramienta de detección	N/A
Activo involucrado:	Plugings de WordPress
Tipo de incidente:	Boletín informativo
Nivel de riesgo:	Alto

Objetivo:

Informar a las entidades del ecosistema Digital sobre la vulnerabilidad CVE-2024-9234 de Carga Arbitraria de Archivos que permite la Ejecución Remota de Código (RCE) en los plugins GutenKit y Hunk Companion de WordPress, que cuentan con más de 40 000 y 8000 instalaciones activas, respectivamente.

Descripción:

Esta es una vulnerabilidad que fue registrada y parcheada en 2024, pero reportes de varias fuentes han informado que desde principios de octubre de 2025 se ha detectado una campaña de explotación masiva y activa. Los atacantes están escaneando sitios de WordPress vulnerables para tomar control de ellos.

Los atacantes están intentando explotar 3 vulnerabilidades de los plugins GutenKit y Hunk Companion las cuales son:

- CVE-2024-9234 : Un error de RCE que permite a atacantes no autenticados instalar y activar plugins arbitrarios, o usar la funcionalidad para subir archivos arbitrarios falsificados como plugins. Tiene una calificación CVSS de 9.8 y afecta a todas las versiones del plugin GutenKit

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

(bloques de creación de páginas, patrones y plantillas para el editor de bloques de Gutenberg), hasta la versión 2.1.0 inclusive.

- CVE-2024-9707 : Una vulnerabilidad crítica que permite a atacantes no autenticados instalar y activar plugins arbitrarios. Estos pueden utilizarse para lograr RCE si se instala y activa otro plugin vulnerable. Este error tiene una puntuación CVSS de 9.8 y afecta a todas las versiones del plugin Hunk Companion para WordPress hasta la 1.8.4 inclusive.
- CVE-2024-11972 : Vulnerabilidad crítica de instalación/activación no autorizada de plugins que afecta a todas las versiones del plugin Hunk Companion para WordPress, hasta la 1.8.5 inclusive. Tiene una puntuación CVSS de 9.8. Se trata de una evasión de CVE-2024-9707 que permite a atacantes no autenticados instalar y activar plugins arbitrarios para RCE si se instala y activa otro plugin vulnerable.

Las vulnerabilidades permiten a los actores de amenazas secuestrar “fácilmente” sitios específicos cargando archivos PHP y ejecutando código malicioso en el servidor, que permite la Ejecución Remota de Código (RCE).

Detalles de la vulnerabilidad:

Impacto: Un atacante que explote esta falla puede subir archivos maliciosos (como *backdoors* o gestores de archivos) al servidor. Esto le otorga al atacante la capacidad de tomar control total del sitio web, robar datos, redirigir a los usuarios a sitios maliciosos o utilizar el servidor para lanzar otros ataques.

Estado: Explotado activamente. Se observó que actores de amenazas explotaban la vulnerabilidad de forma masiva a pesar de que fue reportada en el 2024 están escaneando varios sitios en busca de la existencia de esta vulnerabilidad.

Urgencia: Hay una campaña de "explotación masiva" en curso, lo que significa que los atacantes están buscando y atacando activamente sitios vulnerables ahora mismo.
Además, presenta una puntuación CVSS de 9.8, una de las más altas posibles. Esto se debe a que el ataque es fácil de realizar debido a que no se necesita un nombre de usuario o contraseña, lo que permite cualquier persona en Internet puede lanzar el ataque contra un sitio vulnerable.

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

Vector de ataque: El atacante localiza un sitio de WordPress que utiliza una versión vulnerable del plugin GutenKit o de Hunk Companion. El plugin tiene un punto final (endpoint) en la API REST (/wp-json/gutenkit/v1/install-active-plugin) o (install_and_activate_plugin_from_external())que está destinado a instalar plugins desde un URL externa.

Productos afectados:

Los plugin para WordPress afectados son:

- GutenKit – versión 2.1.0 e inferiores
- Hunk Companion – versión 1.8.5 e inferiores
-

Modo de explotación de la vulnerabilidad

La vulnerabilidad existe debido a una "Comprobación de Capacidad Faltante" (Missing Capability Check) en una de las funciones de la API REST del plugin afectado.

1. Endpoint Vulnerable: El plugin expone un punto final (endpoint) de la API REST diseñado para instalar y activar plugins desde una URL externa (específicamente la función install_and_activate_plugin_from_external()).
2. Falta de Autenticación: Este endpoint no verifica adecuadamente si el usuario que realiza la solicitud tiene permisos de administrador.
3. Vector de Ataque: Un atacante no autenticado (cualquier visitante del sitio) puede enviar una solicitud especialmente diseñada a esta API, ordenando al sitio web que descargue un archivo ZIP desde una URL controlada por el atacante (como un repositorio de GitHub) y lo instale como un nuevo plugin.
4. Compromiso: El archivo ZIP contiene código malicioso (un *backdoor*), que se activa inmediatamente, dando al atacante acceso de administrador y control sobre el sitio.

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

A continuación se presenta un fragmento del código del complemento de GutenKit, se revela que el complemento utiliza la install_and_activate_plugin_from_external()función en la ActivePluginDataclase para administrar las instalaciones de complementos desde fuentes externas a través del gutenkit/v1/install-active-pluginpunto final de la API REST.

```
add_action('rest_api_init', function() {
    register_rest_route('gutenkit/v1', 'install-active-plugin',
        array(
            'methods'             => \WP_REST_Server::EDITABLE,
            'callback'            => [$this, 'install_and_activate_plugin_from_external'],
            'permission_callback' => '__return_true',
        ),
    );
});
```

```
public function install_and_activate_plugin_from_external($request) {
    // The external plugin URL
    $plugin_url = $request->get_param('plugin');
    $slug = $request->get_param('slug');
    $plugin_slug = "$slug/$slug.php";
    $plugin_dir = WP_PLUGIN_DIR;  // This points to wp-content/plugins

    require_once ABSPATH . 'wp-admin/includes/file.php';
    require_once ABSPATH . 'wp-admin/includes/plugin.php';
    require_once ABSPATH . 'wp-admin/includes/class-wp-upgrader.php';

    WP_Filesystem();

    // Download the plugin ZIP file
    $temp_file = download_url($plugin_url);
    if (is_wp_error($temp_file)) {
        wp_send_json_error('Failed to download plugin. Error: ' . $temp_file->get_error
        return;
    }

    $command = "unzip $temp_file -d $plugin_dir";
    exec($command);

    // Unzip the plugin into the wp-content/plugins directory
    $unzip_result = unzip_file($temp_file, $plugin_dir);

    // Delete the temporary file after unzipping
    unlink($temp_file);

    if (is_wp_error($unzip_result)) {
        wp_send_json_error('Failed to unzip plugin. Error: ' . $unzip_result->get_error
        return;
    }

    // Check if the plugin directory exists
    $plugin_path = $plugin_dir . '/' . $plugin_slug;

    if (!file_exists($plugin_path)) {
        wp_send_json_error('The plugin directory does not exist after unzipping.');
        return;
    } else {
        wp_send_json_success('Plugin installed successfully!');
    }
}
```


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

Indicadores de Compromiso

Se recomienda realizar una busqueda en el registro de acceso del sitio las solicitudes que contengan la siguiente petición:

- /wp-json/gutenkit/v1/instalar-complemento-activo
- /wp-json/hc/v1/themehunk-import

También recomendamos revisar los archivos de registro para detectar cualquier solicitud que se origine desde las siguientes direcciones IP:

- 13.218.47.110
- 3.10.141.23
- 52.56.47.51
- 18.219.237.98
- 2600:1f16:234:9300:70c6:9e26:de1a:7696
- 18.116.40.45
- 119.34.179.21
- 2600:1f16:234:9300:f71:cama2:11e5:4080
- 194.87.29.184
- 3.133.135.47
- 3.141.28.47
- 3.85.107.39
- 3.148.175.195
- 193.84.71.244
- 3.147.6.140
- 3.144.26.200
- 193.233.134.136

Dominios involucrados:

- ls.fatec[.]info
- dari-slideshow[.]ru
- zarjavelli[.]ru

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

- korobushkin[.]ru
- drschischka[.]en
- dpaxt[.]io
- cta.imasync[.]com
- catbox[.]moe (sitio web para compartir archivos)

Recomendaciones de mitigación:

La solución principal y más efectiva es actualizar el plugin:

Actualizar: Los administradores del sitio deben actualizar el plugin GutenKit a la versión 2.1.1 o una versión superior, en el plugin de Hunk Companion se requiere instalar la versión 1.9.0 o superior. Esta versión corrige la falla implementando la verificación de permisos adecuada.

En caso de sospechar que el sitio pudo haber sido comprometido, realiza las siguientes acciones:

- Implementa reglas en tu Firewall de Aplicaciones Web (WAF) para bloquear solicitudes al endpoint vulnerable: .../wp-json/gutenkit/v1/install-active-plugin

- Revisa tu directorio wp-content/plugins/ y wp-content/upgrade/ a través de FTP o el gestor de archivos de tu hosting. Busca cualquier plugin o archivo PHP sospechoso que no reconozcas y elimínalo. Los atacantes suelen subir archivos ZIP maliciosos que se hacen pasar por plugins.

- Analiza los registros de acceso de tu servidor web en busca de solicitudes POST al endpoint mencionado anteriormente. Esto puede ayudarte a identificar la dirección IP del atacante y el momento del compromiso.

- Revisa la lista de usuarios administradores en tu WordPress y elimina cualquier cuenta que no hayas creado.

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

Fuentes:

- https://www.wordfence.com/blog/2025/10/mass-exploit-campaign-targeting-arbitrary-plugin-installation-vulnerabilities/
- https://github.com/WordPressBugBounty/plugins-gutenkit-blocks-addon/blob/dc3738bb821cf1d93a11379b8695793fa5e1b9e6/gutenkit-blocks-addon/includes/Admin/Api/ActivePluginData.php#L76
- https://csirt.telconet.net/comunicacion/boletines-servicios/explotacion-masiva-de-vulnerabilidades-criticas-en-plugins-gutenkit-y-hunk-companion-para-wordpress/
- https://www.infosecurity-magazine.com/news/critical-wordpress-plugin-bugs/

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