

Nro. Alerta:	EC-2022-11	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS EcuCERT ALERTA DE SEGURIDAD	
TLP:	 TLP:BLANCO		
Fecha:	22-enero-2022	Vulnerabilidad del Plugin de WordPress Download Monitor	Versión 1.0

I. DATOS GENERALES:

Clase de alerta:	Vulnerabilidad
Tipo de incidente:	Sistema y/o Software Abierto
Nivel de riesgo:	Medio

II. ALERTA

Una vulnerabilidad ha sido detectada en **Download Monitor Plugin**, afectando a las versiones inferiores a 4.4.6 de WordPress Plugin y mediante la manipulación de un input desconocido provoca una vulnerabilidad de *clase cross site scripting (XSS)* en el sitio WEB.

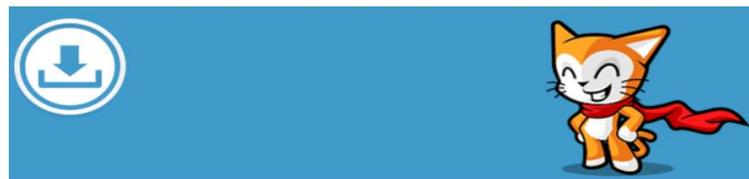


Figura 1.- Ilustraciones representativa de WordPress Download Monitor
Fuente: WordPress

III. INTRODUCCIÓN

Download Monitor es un plugin utilizado para gestionar las descargas en un sitio WEB del ecosistema de WordPress; siendo su uso ampliamente difundido en empresas como WPBeginner, Pagely, Jilt, WP Fusion y Kinsta.

A continuación se mencionan características de la vulnerabilidad asociada a este *plugin*:

Descripción	Detalle
Fecha de publicación	15 de enero de 2022
CVE asociado	CVE-2021-36920
Versiones afectadas	Versiones inferiores a 4.4.6
TOP 10 DE OWASP¹	A7: Secuencias de comandos entre sitios (XSS)

Tabla 1. Características generales de la vulnerabilidad

¹ Es un documento de los diez riesgos de seguridad más importantes en aplicaciones WEB según la organización OWASP (Open Web Application Security Project, Proyecto Abierto de Seguridad de Aplicaciones Web).



Nro. Alerta:	EC-2022-11	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS EcuCERT ALERTA DE SEGURIDAD	
TLP:	 TLP:BLANCO		
Fecha:	22-enero-2022	Vulnerabilidad del Plugin de WordPress Download Monitor	Versión 1.0

IV. VECTOR DE ATAQUE: REMOTO

La Vulnerabilidad de secuencias de comandos entre sitios (XSS) descubierta en el monitor de descarga del complemento de **WordPress Download Monitor** en las versiones inferiores a 4.4.6, permite que un atacante, mediante la manipulación de un input pueda inyectar, un código html y un script arbitrario en el sitio WEB comprometido, alterando la apariencia y permitiendo iniciar nuevos ataques contra el sitio comprometido.

V. IMPACTO

Esta vulnerabilidad afecta a las versiones inferiores a 4.4.6 del *Plugin Download Monitor*; así mismo, existe una afectación de la integridad, provocando que el atacante pueda modificar archivos.

A continuación, se indica la cadena de vectores correspondiente:

Descripción	Detalle
Cadena de Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

Tabla 2. Cadena de Vector

VI. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo, lo siguiente:

- Actualizar el complemento *WordPress Download Monitor* a la última versión disponible; siendo al momento 4.4.7.
- Instalar las actualizaciones del fabricante disponibles en medios oficiales del proveedor.



Nro. Alerta:	EC-2022-11	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS EcuCERT ALERTA DE SEGURIDAD	
TLP:	 TLP:BLANCO		
Fecha:	22-enero-2022	Vulnerabilidad del Plugin de WordPress Download Monitor	Versión 1.0

VII. REFERENCIAS:

- RIST, N. (01 de 2022). NVD RIST. Obtenido de NVD RIST: <https://nvd.nist.gov/vuln/detail/CVE-2021-36920#>
- VULDB. (15 de 01 de 2022). VULDB. Obtenido de VULDB: <https://vuldb.com/?id.190480>
- B. d. (s.f.). Base de datos de vulnerabilidades. Obtenido de Base de datos de vulnerabilidades: <https://patchstack.com/database/vulnerability/download-monitor/wordpress-download-monitor-plugin-4-4-6-authenticated-reflected-cross-site-scripting-xss-vulnerability>
- WordPress. (s.f.). WordPress. Obtenido de WordPress: <https://es.wordpress.org/plugins/download-monitor/>
- WordPress. (s.f.). WordPress. Obtenido de WordPress: <https://wordpress.org/plugins/download-monitor/#description>
- WPSCAN. (14 de 01 de 2022). WPSCAN. Obtenido de WPSCAN: <https://wpscan.com/vulnerability/5b01f184-5bbd-4c8a-b5f6-54d34f46dd1a>

