Nro. Alerta:	AL-2024-023	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR ALERTAS DE SEGURIDAD	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	30-oct-2024	**VULNERABILIDAD XSS EN JANTO TICKETING SOFTWARE**	Pág.: **1** of **4**

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad

Tipo de incidente: Cross Site Scripting

Nivel de riesgo: Medio

II. ALERTA

CVE-2024-10332: se ha encontrado una vulnerabilidad *Cross-Site Scripting* reflejado en el software Janto v4.3r11 desarrollado por la empresa Impronta. Esta vulnerabilidad permite a un atacante ejecutar código JavaScript en el navegador de la víctima enviándole una URL maliciosa utilizando el *endpoint* "/abonados/public/janto/main.php".

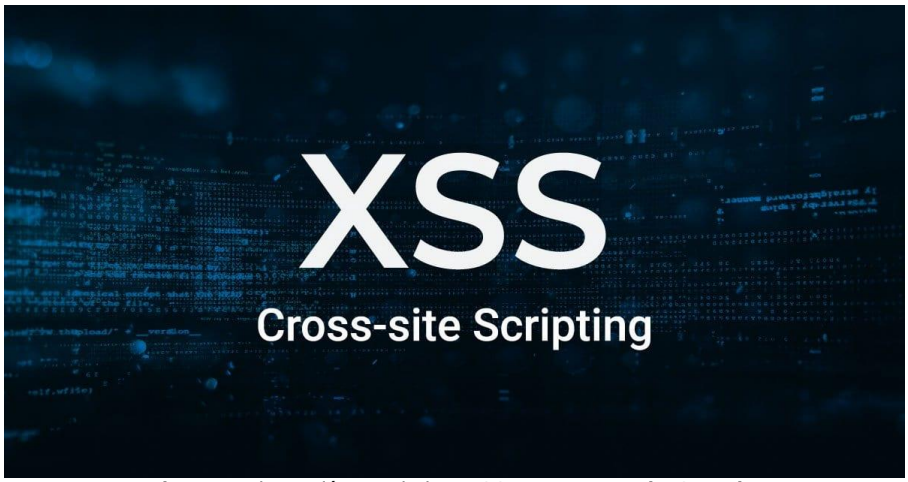

Figura 1.- *Ilustración asociada a XSS* ***Fuente: WeLiveSecurity***

III. INTRODUCCIÓN

Cross Site Scripting, también conocida como XSS, una de las vulnerabilidades más comunes desde 2014. De hecho, según OWASP, esta vulnerabilidad que a partir de este año será incluida dentro de la categoría de inyecciones, forma parte del top 10 de vulnerabilidades más frecuentes en aplicaciones web.

Se trata de un tipo de ataque que aprovecha fallas de seguridad en sitios web y que permite a los atacantes implantar scripts maliciosos en un sitio web legítimo (también víctima del atacante) para ejecutar un script en el navegador de un usuario desprevenido que visita dicho sitio y afectarlo, ya sea robando credenciales, redirigiendo al usuario a otro sitio malicioso, o para realizar defacement en un sitio web.

IV. VECTOR DE ATAQUE:

Para la vulnerabilidad presentada se ha considerado la siguiente métrica:

Recursos Afectados: Janto Ticketing Software versión 4.3r11.

CVSS v3.1 Severidad y Métricas:

Puntuación base:	6.10 Media
Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Vector de Acceso (AV):	A través de red
Complejidad de Acceso (AC):	Bajo
Privilegios requeridos (PR):	Ninguno
Interacción del usuario (UI):	Obligatorio
Alcance (S):	Modificado
Impacto a la Confidencialidad (C):	Bajo
Impacto a la Integridad (I):	Bajo
Impacto a la disponibilidad (A):	Ninguno

V. INDICADORES DE COMPROMISO

En el caso presentado se ha podido ver que el ataque se puede catalogar como un Robo de sesión, considerando que en el supuesto caso de que las cookies de sesión no estén protegidas, mediante un ataque XSS se puede leer la cookie de sesión de la víctima y enviarla a un servidor controlado por el atacante. Con esto, el atacante podrá acceder a la web del mismo modo que el usuario y realizar todas las acciones que el usuario pueda realizar.

VI. IMPACTO:

- Redirigir a los usuarios a un sitio web malicioso.
- Capturar las teclas que presionan los usuarios.
- Acceder al historial del navegador de los usuarios y al contenido del portapapeles.
- Ejecutar exploits basados en navegador web (por ejemplo, bloquear el navegador). En este caso la dirección URL maliciosa utilizada es: *endpoint* "/abonados/public/janto/main.php".

VII. RECOMENDACIONES:

- Lo principal y fundamental para evitar ser vulnerable a este tipo de ataques, es contar con soluciones de seguridad instaladas y correctamente actualizadas**.** Esta parte es muy importante debido a que si se ejecuta algún *malware* o código malicioso en el equipo al acceder a un sitio web vulnerable, estas soluciones que contengan las últimas firmas sean capaces de bloquearlas.

- Adicionalmente, es posible que se aprovechen este tipo de ataques, para crear redirecciones a sitios que contengan algún tipo de phishing**,** en este caso, las protecciones de los antivirus cuentan con el bloqueo a este tipo de sitios y también el bloqueo por parte de los navegadores web.

- Es primordial siempre vigilar los sitios, observar la dirección URL a la que se accede, ya que en este caso podremos identificar las redirecciones no controladas y aprovechadas por estos ataques, que podrían ser aprovechadas por los atacantes.

- También existen complementos o extensiones para nuestros navegadores web, encargados de bloquear y mitigar la ejecución de estos scripts maliciosos.

- Se recomienda la extensión ***NoScript***, la cual permite realizar configuraciones personalizadas.

- Por último**,** se recomienda utilizar navegadores alternativos, es decir, no tan populares**,** como pueden ser Opera, Comodo o Chromium. De este modo, si un usuario malicioso envía un ataque que intente explotar alguna deficiencia o vulnerabilidad, normalmente será para los navegadores más conocidos y al no darse las condiciones para la ejecución de la vulnerabilidad, no podrá explotarse correctamente.

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:

- https://impronta.es/
- https://www.incibe.es/en/incibe-cert/notices/aviso/cross-site-scripting-xss-vulnerability-janto-impronta
- https://seguridad.prestigia.es/que-es-un-cross-site-scripting-y-como-afecta-a-tu-web/
- https://www.a2secure.com/blog/los-peligros-de-los-ataques-de-cross-site-scripting-xss/
- https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2024-10332
- https://nvd.nist.gov/vuln/detail/CVE-2024-10332