BOLETÍN DE ALERTA

Boletín Nro.: 2022-12

Fecha de publicación: 25/02/2022

Tema: Vulnerabilidad Cross-Site Scripting (XSS) en *Horde webmail* client.

Software afectado:

- Horde webmail client 5.2.22

Descripción:

Se ha detectado una vulnerabilidad en *Horde webmail* que permitiría a un atacante realizar ejecución de código JavaScript en el sistema vulnerable.

Esta vulnerabilidad se debe a un error en el componente utilizado para visualizar documentos *OpenOffice* en HTML llamado *XSLT* (*eXtensible Stylesheet Language Transformations*), el cual no controla correctamente estos documentos. Esto permitiría a un atacante crear un documento malicioso de *OpenOffice* con el objetivo de realizar ejecución de código JavaScript en el sistema vulnerable.

Impacto:

La falla de seguridad puede dar acceso a un atacante a toda la información que la víctima posee almacenado en su correo electrónico, lo cual podría permitirle el acceso a información sensible o acceso a los servicios internos de una organización.

Detección:

Comprobar si posee la versión del software vulnerable (5.2.22) instalado en el equipo utilizando el siguiente comando:

- *cat /var/cpanel/horde/version*

Solución:

Actualmente el fabricante no ha lanzado ninguna actualización de seguridad que subsane dicha vulnerabilidad, sin embargo, investigadores recomiendan como método de mitigación temporal, añadir la configuración *"disable => true"* a la opción ***OpenOffice mime handler*** que se encuentra en el archivo de configuración "*config/mime_drivers.php*" del *Horde webmail client.*

Información adicional:

- https://thehackernews.com/2022/02/9-year-old-unpatched-email-hacking-bug.html
- https://www.covertswarm.com/post/0-day-vulnerability-in-horde-webmail-email-system
- https://portswigger.net/daily-swig/zero-day-xss-vulnerability-in-horde-webmail-client-can-be-triggered-by-file-preview-function