Se han revelado dos vulnerabilidades de seguridad en el conjunto de servidores de correo de código abierto Mailcow que podrían ser explotadas por actores maliciosos para ejecutar código arbitrario en instancias vulnerables.

Ambas fallas afectan a todas las versiones del software anteriores a la versión 2024-04, lanzada el 4 de abril de 2024. Los problemas fueron divulgados de manera responsable por SonarSource el 22 de marzo de 2024.

Las vulnerabilidades, clasificadas como de severidad Moderada, son las siguientes:

- CVE-2024-30270 (puntaje CVSS: 6.7) – Una vulnerabilidad de recorrido de directorios que afecta a una función llamada «rspamd_maps()», la cual podría permitir a un atacante ejecutar comandos arbitrarios en el servidor al sobrescribir cualquier archivo que pueda ser modificado por el usuario «www-data».
- CVE-2024-31204 (puntaje CVSS: 6.8) – Una vulnerabilidad de scripting entre sitios (XSS) a través del mecanismo de manejo de excepciones cuando no se está operando en el modo DEV_MODE.

La segunda vulnerabilidad se debe a que guarda los detalles de las excepciones sin ningún tipo de sanitización o codificación, que luego se renderizan en HTML y se ejecutan como JavaScript en el navegador de los usuarios.

Como resultado, un atacante podría explotar esta falla para inyectar scripts maliciosos en el panel de administración provocando excepciones con entradas especialmente diseñadas, permitiéndoles secuestrar la sesión y realizar acciones privilegiadas como administrador.

En otras palabras, al combinar ambas fallas, una parte malintencionada podría tomar el control de cuentas en un servidor Mailcow y obtener acceso a datos sensibles, así como ejecutar comandos.

En un escenario teórico de ataque, un atacante podría crear un correo electrónico HTML que

contenga una imagen de fondo en CSS cargada desde una URL remota, utilizándola para activar la ejecución de una carga útil XSS.

> *«Un atacante puede combinar ambas vulnerabilidades para ejecutar código arbitrario en el servidor del panel de administración de una instancia vulnerable de Mailcow»*, dijo Paul Gerste, investigador de vulnerabilidades de SonarSource.
>
> *«Para que esto ocurra, un usuario administrador debe visualizar un correo electrónico malicioso mientras está conectado al panel de administración. La víctima no tiene que hacer clic en un enlace dentro del correo ni realizar ninguna otra interacción con el mismo; solo debe continuar usando el panel de administración después de ver el correo.»*