

CVE-2026-34040

Body >1MB

CRACK

Huge API request

AuthZ plugin

شنو هاد
CVE-2026-34040؟

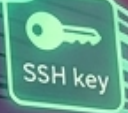
body ال
تجاوز 1MB!؟



BOOM



هاها دخلت لل
!host



```
docker API:  
/containers/create
```



صاوب
privileged
container!



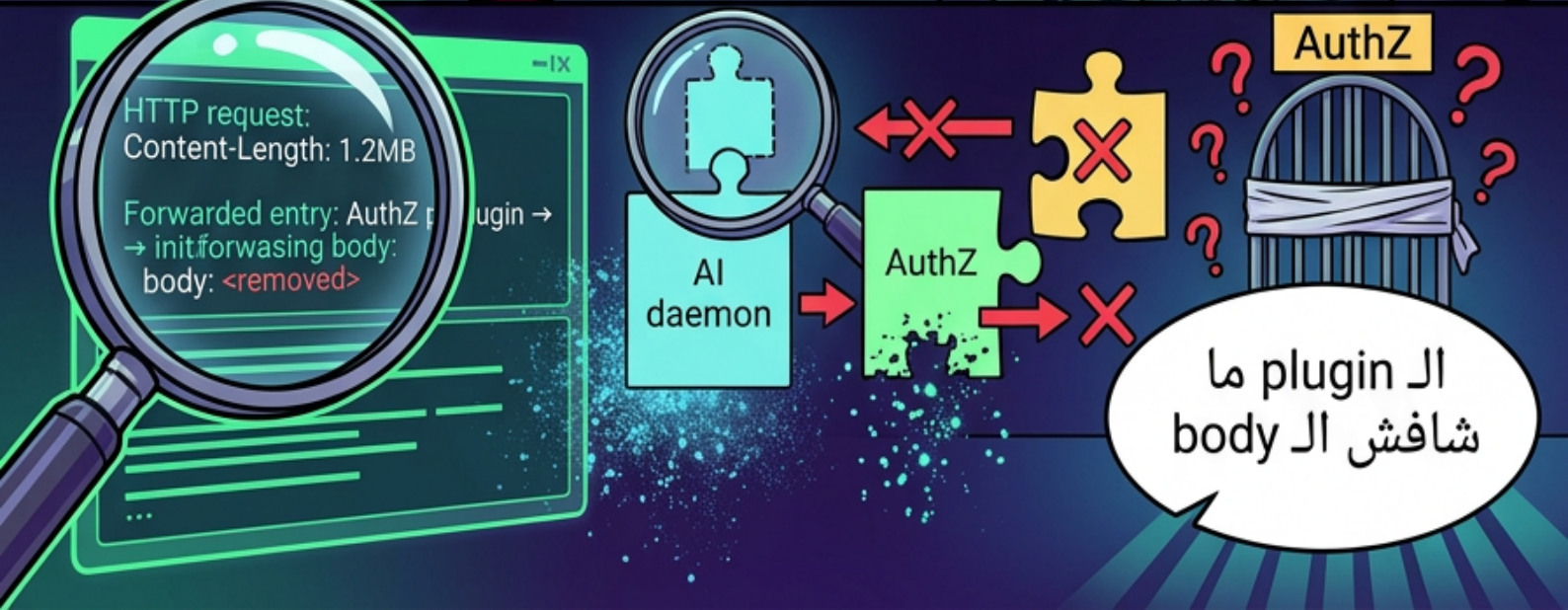
```
docker API: /containers/create  
seccan den:-:ound (  
  codes "onoo"  
  *Boecher APs: /containers/create  
  return -1;  
)
```





شنو وقع ف AuthZ؟

```
HTTP request:  
Content-Length: 1.2MB  
  
Forwarded entry: AuthZ plugin  
→ initforwaioing body:  
body: <removed>
```



شافش ال plugin ما body ال

Patched: CVE-2026-34040

حدّث Docker
لنسخة 29.3.1 دابا!

UPDATE

PATCH APPLIED

CVE-2026-34040 fixed

🔒 Tips

- Rootless
- Usersn-remap
- Limit API access

29.3.1

KRASH!

خدم Rootless و
!least-privilege