

شنو هاد
CVE-2026-39987؟



09:41
9h41m
توڤيع
CVE-2026-39987

تتبيه!
استغلال ممكن
ف /terminal/ws

MAS

```
validate_auth() missing
```

```
curl -XPOST http://localhost:8080/terminal/ws
```

```
{  
  "name": "root",  
  "found": true,  
  "id": "1"
```



```
Files
├── files
│   └── files
│       ├── snoptots
│       │   └── det
│       │       ├── .env
│       │       ├── .new
│       │       └── invariables
│       │           └── SSH keys
│       ├── hors
│       ├── fanctiens
│       └── rastterot
```

```
File Trees
├── exfiltration
├── achecots
├── servers
├── mans
├── ower.
└── command executed
```

```
Terminal
[ 27:27:27:35:11 ] [::alarm] : PTY allocated
[ 27:27:27:36:19 ] [::] : command executed
[ 27:27:27:36:19 ] [::] : command executed
```

```
Terminal
> cd /
> ls -la
```

```
Timeline
Sun Sun Tue Wed Thu 24 25 26 27 28 29 30 31 40
[ 27:27:27:35:11 ] [::alarm] : PTY allocated
[ 27:27:27:36:19 ] [::] : command executed
[ 27:27:27:36:19 ] [::] : command executed
```

سرقو .env. و مفاتيح SSH!

دخلوا ف أقل من 10 سوابع!

Sysdig لاحظ
الهجوم في
honeypot ال

ما كانش
منشور، هاك
خدم يدويًا

ATTACK TIMELINE (90 minutes)

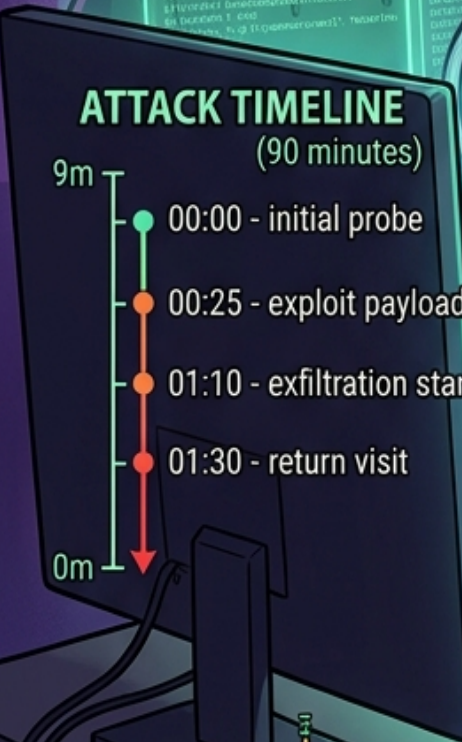
- 9m
- 00:00 - initial probe
- 00:25 - exploit payload
- 01:10 - exfiltration start
- 01:30 - return visit
- 0m



RECON

MANUALLY OPERATED

EXFIL



.env

ssh id_rsa

ssh id_rsa

```
grep auth_hellora
grep auth_failure
```

Exfiltration

- Websocket frames
- Authorization: null
- websocket frames
- Authorization: null
- websocket frames
- Authorization: null
- websocket frames
- Authorization: null
- websocket frames
- Authorization: null
- websocket frames
- Authorization: null

Data exfiltration

- Manually operated value
- Access denied
- Access - return visit

Marimo
0.23.0

Marimo
0.23.0

حدثول
Marimo 0.23.
دابا!

Patch applied 100%

Patch applied
validate_auth() enforced

closed
closed

0.23.0

حدثول
Marimo 0.23.0
دابا!

/terminal/ws

SHICK

سدو /terminal/ws
و فعلو
authentication !

0.23.0

WHOOOSH