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

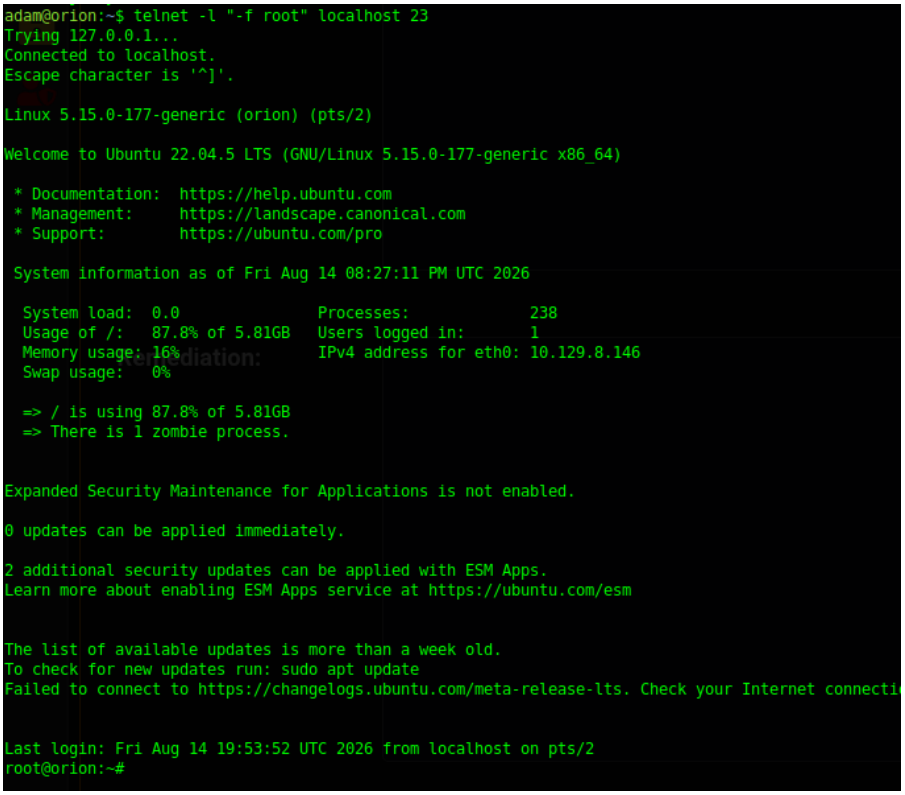

Figure 1. root.png

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

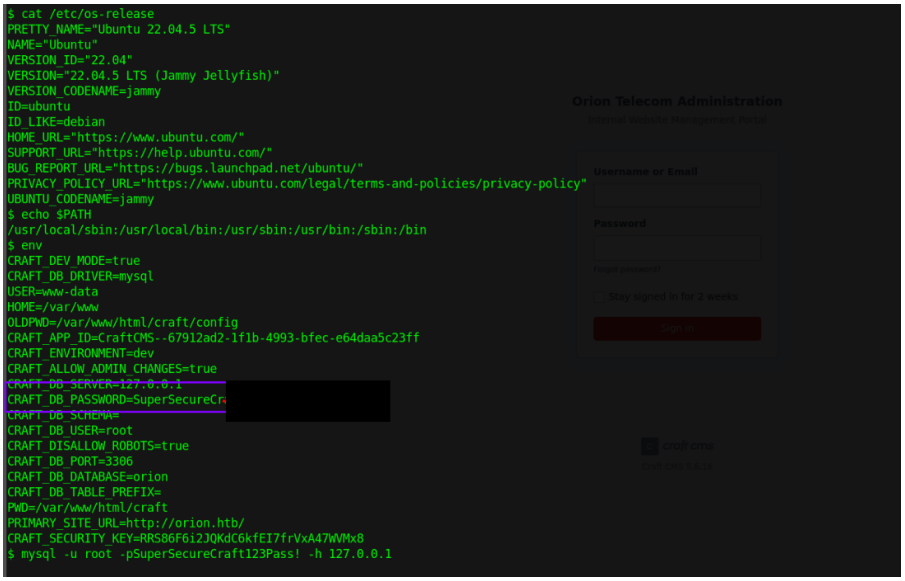

Figure 2. env_command.png

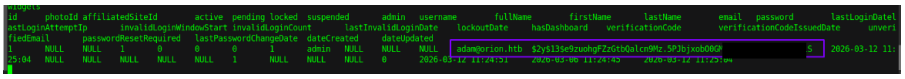

Figure 3. mysql_adam_user.png

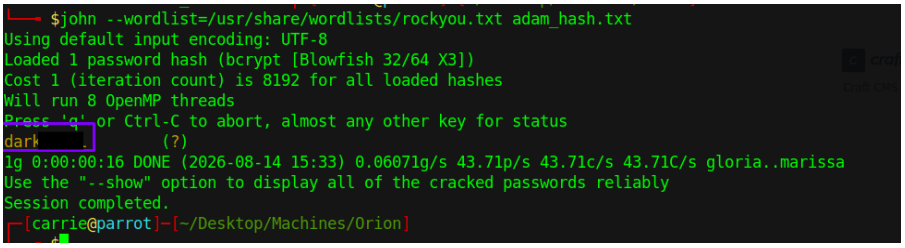

Figure 4. adam_cracked.png

Background

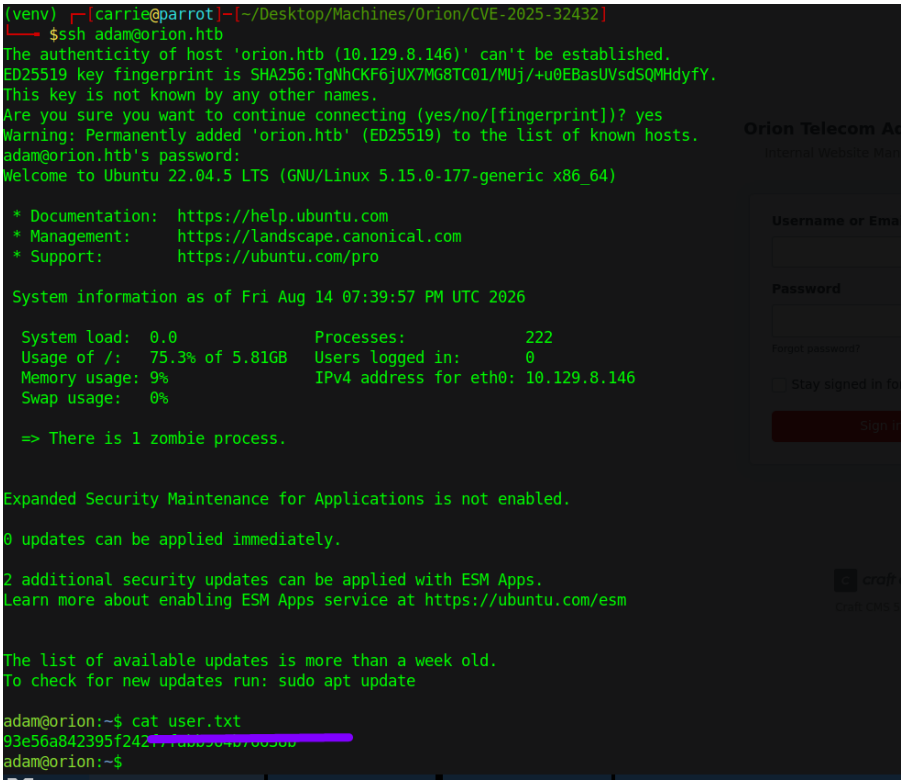

Figure 5. user_txt.png

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	

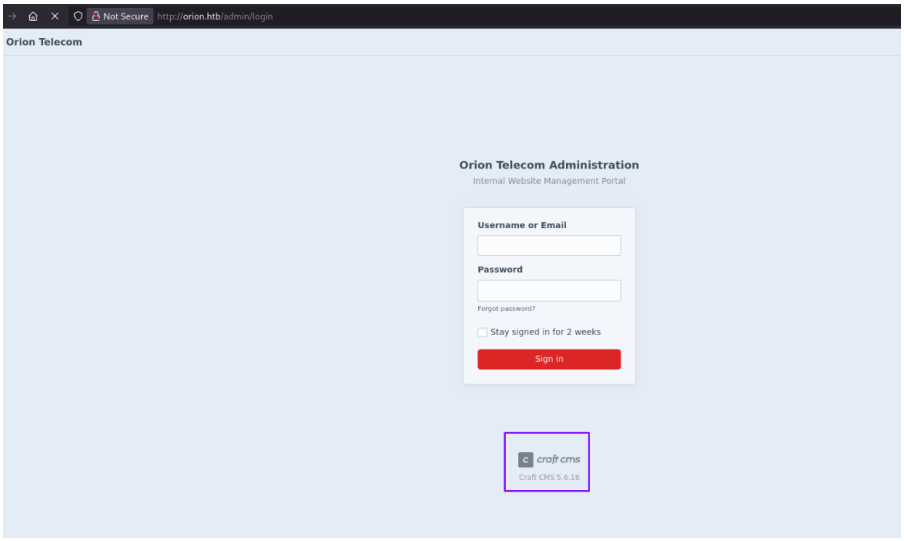

Figure 6. craft_sms.png

Background

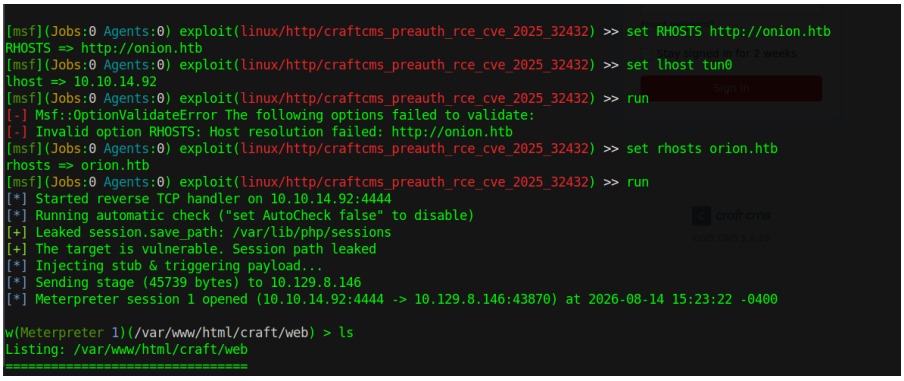

Figure 7. rce.png

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)

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