



# Recently there were several reports on the following: Security: CVE-2026-41940 - cPanel & WHM / WP2 Security Update 04/28/2026



Sign in

cPanel > cPanel & WHM > Support Topics > Security

Search

Articles in this section

Your browser version needs an update for this banner to work properly.

### Privacy Settings

This site uses third-party website tracking technologies to provide and continually improve our services, and to display advertisements according to users' interests. I agree and may revoke or change my consent at any time with effect for the future.

[Privacy Policy](#) [Legal Notice](#) [More Information](#)

Deny

Accept All

Powered by Usercentrics Consent Management

### Latest Article Changes:

*04/29/26 02:46PM CST: Updated article's required actions and added detection script.*

*04/28/26 04:36PM CST: Updated article to include patched versions.*

*04/28/26 03:19PM CST: Updated article to reflect changes in mitigation steps*

*04/28/26 12:05PM CST: Initial article published.*

## Cause

An authentication bypass security issue has been identified in the cPanel software (including DNSOnly) affecting all versions after 11.40.

## Resolution

We have pushed out a patch for the following cPanel & WHM versions:

- 11.86.0.41
- 11.110.0.97
- 11.118.0.63
- 11.126.0.54
- 11.130.0.18
- 11.132.0.29
- 11.136.0.5
- 11.134.0.20

We have pushed out a patch for the following WP Squared version:

- 136.1.7



Your browser version needs an update for this banner to work properly.

### Privacy Settings

This site uses third-party website tracking technologies to provide and continually improve our services, and to display advertisements according to users' interests. I agree and may revoke or change my consent at any time with effect for the future.

[Privacy Policy](#) [Legal Notice](#) [More Information](#)

Powered by Usercentrics Consent Management

```
/usr/local/cpanel/cpanel -V
```

```
/scripts/restartsrv_cpssrvd
```

3. Please note that if you have disabled cPanel updates or pinned your cPanel update configuration to a specific version, then these will not auto-update. Please identify and update these servers manually as a priority. Information on how to customize cPanel's Update Preferences from the Command line can be found via the following support article:

[How to customize cPanel's Update Preferences from the Command Line](#)

4. In cases where you are not able to perform the above resolution, please apply one of the following mitigations:

- Block inbound traffic on ports 2083, 2087, 2095, and 2096 at the firewall. **Or,**
- Stop cpsrvd and cpdavd:

```
whmapi1 configureservice service=cpsrvd enabled=0 monitored=0 &&
```

We are currently working on finding paths to get a patch to versions not included above, especially for versions that have higher quantities of servers. In the meantime, it is highly recommended that you follow the instructions below until you can update to a supported version above that will continue to be updated as we release patches.



**Warning: If your server is not running a supported version of cPanel that is eligible for this update, it is highly recommended that you work toward updating your server as soon as possible, as it may also be affected.**



Your browser version needs an update for this banner to work properly.

### Privacy Settings

This site uses third-party website tracking technologies to provide and continually improve our services, and to display advertisements according to users' interests. I agree and may revoke or change my consent at any time with effect for the future.

[Privacy Policy](#) [Legal Notice](#) [More Information](#)

Powered by Usercentrics Consent Management

```
#!/bin/bash
# Scan for compromised session files

SESSIONS_DIR="/var/cpanel/sessions"
COMPROMISED=0

echo "[*] Scanning session files for injection indicators..."

for session_file in "$SESSIONS_DIR"/raw/*; do
  [ -f "$session_file" ] || continue
  session_name=$(basename "$session_file")

  # Check if this session is/was pre-auth
```

```
preauth_file="$SESSIONS_DIR/preauth/$session_name"

# IOC 0: Session has both token_denied AND cp_security_token and
#
# token_denied is set by do_token_denied() in cpsrvd when a request
# supplies an incorrect security token. cp_security_token is the
# attacker-injected token value. This combination indicates:
#
# 1. Attacker injected a cp_security_token via newline payload
# 2. Attacker attempted to use the injected token
# 3. cpsrvd recorded the token mismatch (token_denied counter)
#    during the exploitation window before the session was
#    fully promoted
#
```



Your browser version needs an update for this banner to work properly.

## Privacy Settings

This site uses third-party website tracking technologies to provide and continually improve our services, and to display advertisements according to users' interests. I agree and may revoke or change my consent at any time with effect for the future.

[Privacy Policy](#) [Legal Notice](#) [More Information](#)

Powered by Usercentrics Consent Management

```
# Extract values for usage context
token_val=$(grep '^cp_security_token=' "$session_file" | head -1)
denied_val=$(grep '^token_denied=' "$session_file" | head -1)
origin=$(grep '^origin_as_string=' "$session_file" | head -1)
used=$(grep -a "$token_val" /usr/local/cpanel/logs/access_log)
external_auth=$(grep '^successful_external_auth_with_timestamp=' "$session_file")

# High confidence if origin is badpass (session was pre-auth)
if grep -q '^origin_as_string=.*method=badpass' "$session_file"; then
    if [ -z "$external_auth" ] && [ -z "$used" ]; then
        echo "Found possible injected session file:"
        echo "  - No sign of usage"
    else
        echo "[!] CRITICAL: Exploitation artifact - token_val=$token_val, denied_val=$denied_val, origin=$origin, used=$used, external_auth=$external_auth"
    fi
fi
```

```
    echo "    - cp_security_token=$token_val"
    echo "    - token_denied=$denied_val"
    echo "    - origin=$origin"
    echo "    - Verdict: Session was pre-auth (badpa
    echo "    - USED: $used"
    COMPROMISED=1
fi
# Medium confidence but still suspicious for any session
else
    echo "[!] WARNING: Suspicious session with token_denied
    echo "    - cp_security_token=$token_val"
    echo "    - token_denied=$denied_val"
    echo "    - origin=$origin"
    echo "    - Review manually: may be legitimate token exp
```



Your browser version needs an update for this banner to work properly.

## Privacy Settings

This site uses third-party website tracking technologies to provide and continually improve our services, and to display advertisements according to users' interests. I agree and may revoke or change my consent at any time with effect for the future.

[Privacy Policy](#) [Legal Notice](#) [More Information](#)

Powered by Usercentrics Consent Management

```
# IOC 2: Any session with tfa_verified but no valid origin
if grep -q '^tfa_verified=1' "$session_file" && \
    ! grep -q '^origin_as_string=.*method=handle_form_login' "$se
    ! grep -q '^origin_as_string=.*method=create_user_session' "$s
    ! grep -q '^origin_as_string=.*method=handle_auth_transfer' '
    echo "[!] WARNING: Session with tfa_verified but suspicious
    COMPROMISED=1
fi

# IOC 3: Password field containing newlines (corrupted session f
if grep -qP '^pass=.*\n.' "$session_file" 2>/dev/null; then
    echo "[!] CRITICAL: Multi-line pass value detected: $session
```

```
COMPROMISED=1
fi
done

if [ "$COMPROMISED" -eq 0 ]; then
    echo ""
    echo "[+] No indicators of compromise found."
else
    echo ""
    echo "[!] INDICATORS OF COMPROMISE DETECTED - IMMEDIATE ACTION REQUIRED"
    echo "    1. Purge all affected sessions"
    echo "    2. Force password reset for root and all WHM users"
    echo "    3. Audit /var/log/wtmp and WHM access logs for unauthorized access"
    echo "    4. Check for persistence mechanisms (cron, SSH keys, etc.)"
```



Your browser version needs an update for this banner to work properly.

### Privacy Settings

This site uses third-party website tracking technologies to provide and continually improve our services, and to display advertisements according to users' interests. I agree and may revoke or change my consent at any time with effect for the future.

[Privacy Policy](#) [Legal Notice](#) [More Information](#)

Powered by Usercentrics Consent Management

```
# /bin/bash ./ioc_checksessions_files.sh
[*] Scanning session files for injection indicators...
[!] CRITICAL: Exploitation artifact - token_denied with injected cp_
- cp_security_token=/cpsess04396539398
- token_denied=1
- origin=address=100.96.3.23,app=whostmgrd,method=badpass
- Verdict: Session was pre-auth (badpass origin) with attacker-injected token
[!] WARNING: Session with tfa_verified but suspicious origin: /var/cpanel/

[!] INDICATORS OF COMPROMISE DETECTED - IMMEDIATE ACTION REQUIRED
    1. Purge all affected sessions
    2. Force password reset for root and all WHM users
    3. Audit /var/log/wtmp and WHM access logs for unauthorized access
```


4. Check for persistence mechanisms (cron, SSH keys, backdoors)  
File: ioc\_checksessions\_files.sh



Was this article helpful?

20 out of 31 found this helpful

## Have more questions?

 Your browser version needs an update for this banner to work properly.

### Privacy Settings

This site uses third-party website tracking technologies to provide and continually improve our services, and to display advertisements according to users' interests. I agree and may revoke or change my consent at any time with effect for the future.

[Privacy Policy](#) [Legal Notice](#) [More Information](#)

Powered by Usercentrics Consent Management

AutoSSL excludes www for new accounts

LFD is stopped and does not start automatically after cPanel version upgrades

## Comments

0 comments

Article is closed for comments.

cPanel



Your browser version needs an update for this banner to work properly.

### Privacy Settings

This site uses third-party website tracking technologies to provide and continually improve our services, and to display advertisements according to users' interests. I agree and may revoke or change my consent at any time with effect for the future.

[Privacy Policy](#) [Legal Notice](#) [More Information](#)

Powered by Usercentrics Consent Management