INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-01 13:38 UTC

CVE-2025-66430: Critical Privilege Escalation in Plesk Allows Root-Level Access

CVE VULNERABILITY | HIGH | CVSS 8.8

SCC Item ID	SCC-CVE-2026-0249
Type	CVE Vulnerability
CVE ID	CVE-2025-66430
Severity	HIGH
CVSS Base Score	8.8
EPSS Score	0.0004 (13th percentile)
Affected Products	Plesk (Password Protected Directories feature); specific version range not confirmed from available sources
Published	4 hours ago
Discovery Source	Serper

Executive Summary

A high-severity privilege escalation vulnerability in Plesk's Password Protected Directories feature allows any low-privileged user on a Plesk-managed server to gain full root-level control of that server. Plesk is widely used by hosting providers and web operations teams to manage websites and server infrastructure; a successful exploit gives an attacker unrestricted access to every site, database, and credential stored on the affected host. Plesk's official advisory and Belgium's Centre for Cybersecurity recommend immediate patching; unpatched servers remain at direct risk of complete compromise.

Technical Analysis

CVE-2025-66430 is a high-severity privilege escalation vulnerability (CVSS 8.8) in Plesk's Password Protected Directories feature. The flaw is classified under CWE-269 (Improper Privilege Management) and CWE-78 (Improper Neutralization of Special Elements used in an OS Command, OS Command Injection), mapping to MITRE ATT&CK techniques T1059 (Command and Scripting Interpreter) and T1068 (Exploitation for Privilege Escalation). A low-privileged authenticated Plesk user can leverage this flaw to execute arbitrary OS-level commands, ultimately achieving root access to the underlying server. The precise technical mechanism, whether direct command injection into the Password Protected Directories feature, improper permission enforcement, or a related code path, is not fully disclosed in publicly available sources as of this writing. CVSS base score 8.8 is from NVD; vendor CVSS score is pending publication. Affected version range is available in

Plesk's official support advisory (support.plesk.com/hc/en-us/articles/36261922405015); consult that source for your deployment version. EPSS score is 0.043% (13th percentile), indicating low observed exploitation activity to date, but the severity and attack vector warrant immediate remediation. Not currently listed in CISA's Known Exploited Vulnerabilities (KEV) catalog as of this writing; no CISA advisory detected. Patch is available per Plesk's official advisory.

Action Checklist

1. Step 1: Containment. Identify all Plesk-managed servers in your environment immediately. Consult Plesk's support advisory (support.plesk.com/hc/en-us/articles/36261922405015) to confirm which versions in your environment are affected. Restrict access to the Plesk control panel to trusted IP ranges only, using firewall rules or Plesk's built-in IP restriction settings (NIST AC-17 Remote Access, CIS 4.4 Implement and Manage a Firewall on Servers). Disable the Password Protected Directories feature in Plesk if it is not operationally required until the patch is applied.
2. Step 2: Detection. Review Plesk server authentication logs and system-level audit logs for unexpected privilege escalation events, root-level command execution by non-root Plesk users, or anomalous use of the Password Protected Directories feature. Query for OS-level commands executed under the Plesk service context outside normal administrative workflows (NIST AU-6 Audit Record Review, Analysis, and Reporting; CIS 8.2 Collect Audit Logs). Check for new cron jobs, modified sudoers entries, added SSH authorized_keys, or new accounts with elevated privileges (D3-LAM Local Account Monitoring, D3-SFA System File Analysis).
3. Step 3: Eradication. Apply the official Plesk patch per Plesk support advisory CVE-2025-66430 (support.plesk.com/hc/en-us/articles/36261922405015), confirming the patched version applicable to your deployment. Verify the installed Plesk version matches the patched version specified in the advisory. Re-enable the Password Protected Directories feature only after patching is confirmed. Rotate all credentials for accounts that had access to the Plesk panel on potentially exposed servers (D3-CRO Credential Rotation, D3-CH Credential Hardening; NIST AC-2 Account Management).
4. Step 4: Recovery. After patching, validate that the Plesk version string reflects the patched release. Audit all local accounts and sudo configurations on affected servers for unauthorized additions or modifications (NIST AC-6 Least Privilege, CIS 5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts, D3-UAP User Account Permissions). Review web application and server audit logs for signs of post-exploitation activity, data exfiltration, backdoor installation, or lateral movement, going back at least 30 days (NIST AU-11 Audit Record Retention). Monitor root-level activity for 30 days post-remediation using SIEM alerting.
5. Step 5: Post-Incident. Assess whether the Password Protected Directories feature, or similar low-privilege user-facing features, were included in your last threat model review. Implement least-privilege access controls on all Plesk user accounts, limiting who can access sensitive features (NIST AC-6, CIS 5.4). Establish automated patch notification monitoring for Plesk advisories. Review your vulnerability management process to ensure hosting control panel software is included in regular patch cycles (CIS 7.1 Establish and Maintain a Vulnerability Management Process, CIS 7.3 Perform Automated Operating System Patch Management). Evaluate separation of duties for multi-tenant Plesk environments (NIST AC-5 Separation of Duties).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to senior IR leadership and legal/compliance counsel immediately if forensic review of /var/log/plesk/panel.log or auditd output confirms any non-root Plesk subscriber account executed commands as root, accessed /etc/shadow, read database credential files, or initiated outbound connections from the server — any of these indicators confirm successful exploitation and trigger breach notification assessment obligations under applicable data protection regulations (GDPR, CCPA, HIPAA) given that Plesk-managed servers typically host multi-tenant web applications with PII and database credentials.
Recovery Notes	After patching to the CVE-2025-66430-remediated Plesk release, validate that the Password Protected Directories feature's underlying file permission logic has been corrected by creating a test subscriber account and confirming it cannot escalate to root via the feature's original attack vector — document this validation test result. Monitor /var/log/audit/audit.log (via auditd rule targeting UID 0 execve events with auid != 0) for a minimum of 30 days post-remediation, as attackers who achieved root access before containment may have implanted cron-based or init.d-based persistence mechanisms that will not surface until triggered. Given that Plesk servers in hosting environments contain credentials for every hosted site's database and application, assume all database passwords, FTP credentials, and application API keys stored in Plesk's configuration (/var/www/vhosts/*/conf/ and Plesk's internal database) are compromised and rotate them as a precautionary measure even in the absence of confirmed exploitation evidence.
Forensic Artifacts	/var/log/plesk/panel.log — Contains timestamped API calls to the Password Protected Directories feature; look for 'passwd_protect' actions initiated by subscriber-tier accounts (non-admin UIDs) as the primary indicator of CVE-2025-66430 exploitation attempts. | /var/log/audit/audit.log (auditd) — EXECVE and SYSCALL records showing uid=0 (root) command execution where auid (audit UID, the original login UID) belongs to a Plesk subscriber account, confirming successful privilege escalation from a low-privileged Plesk user to root. | /var/www/vhosts/*/httpdocs/.htpasswd files — The Password Protected Directories feature manages these files; forensically relevant for attacker-injected htpasswd entries, unexpected modification timestamps, or entries referencing accounts not provisioned through Plesk's normal workflow. | /root/.ssh/authorized_keys and /var/www/vhosts/*/.ssh/authorized_keys — Post-exploitation persistence artifact; an attacker with root access via CVE-2025-66430 would likely add an SSH public key here to maintain persistent access independent of Plesk credentials. | /etc/sudoers and /etc/sudoers.d/* — Modification of sudoers files is a high-confidence post-exploitation persistence indicator; diff these files against a pre-incident baseline to identify NOPASSWD entries or wildcard rules added for Plesk subscriber account usernames.

Per-Action IR Details

Step 1: Containment — Identify all Plesk-managed servers in your environment immediately. Restrict access to the Plesk control panel to trusted IP ranges only, using firewall rules or Plesk's built-in IP restriction settings (aligned with NIST AC-17 Remote Access and CIS 4.4 Implement and Manage a Firewall on Servers). Disable the Password Protected Directories feature in Plesk if it is not operationally required until the patch is applied.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST AC-17 (Remote Access), NIST AC-3 (Access Enforcement), NIST IR-4 (Incident Handling), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: Run 'plesk bin panel_gui --disable' to take the Plesk UI offline immediately if IP restriction cannot be applied in time. On Linux, use iptables to restrict port 8443 (Plesk HTTPS panel) to trusted admin IPs only: 'iptables -I INPUT -p tcp --dport 8443 ! -s -j DROP'. Enumerate all Plesk servers via your internal DNS or hosting inventory using 'grep -r plesk /etc/hosts' or by querying your CMDB export. On each server, disable the Password Protected Directories feature via CLI: 'plesk bin passwd_protect --disable-feature'.

Evidence: Before restricting access, snapshot the current Plesk panel IP allowlist from /etc/sw/keys/ and Plesk's panel.ini (typically /usr/local/psa/admin/conf/panel.ini) to establish the pre-incident access configuration. Capture active TCP connections to port 8443 using 'ss -tnp sport = :8443' or 'netstat -tnp | grep 8443' to identify any sessions in progress from unexpected IPs. Export current /etc/passwd, /etc/shadow, and /etc/sudoers at this moment as a pre-containment baseline before any attacker persistence mechanisms can be cleaned.

Step 2: Detection — Review Plesk server authentication logs and system-level audit logs for unexpected privilege escalation events, root-level command execution by non-root Plesk users, or anomalous use of the Password Protected Directories feature. Query for OS-level commands executed under the Plesk service context outside normal administrative workflows (aligned with NIST AU-6 Audit Record Review, Analysis, and Reporting and CIS 8.2 Collect Audit Logs). Check for new cron jobs, modified sudoers entries, added SSH authorized_keys, or new accounts with elevated privileges (aligned with D3-LAM Local Account Monitoring and D3-SFA System File Analysis).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-2 (Event Logging), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Query Plesk's own panel log at /var/log/plesk/panel.log for references to 'passwd_protect' or 'htpasswd' combined with any user other than root or the assigned domain owner. On Linux, run 'ausearch -m EXECVE -ts today | grep -E "(passwd_protect|htpasswd|sudo|su\b)"' using auditd to find privilege-escalation-related command execution. Check /var/log/auth.log (Debian/Ubuntu) or /var/log/secure (RHEL/CentOS) for 'session opened for user root' events preceded by a non-root Plesk subscriber account. Run 'find /var/spool/cron /etc/cron.d /etc/cron.daily -newer /usr/local/psa/admin/conf/panel.ini -ls' to identify cron entries created or modified after the Plesk configuration timestamp. For sudoers tampering, run 'visudo -c' and diff /etc/sudoers against a known-good backup.

Evidence: Collect /var/log/plesk/panel.log and /var/log/plesk/sw-cp-serverd.log covering at least 30 days, filtering for 'passwd_protect', 'htpasswd', and any API calls to the Password Protected Directories endpoints. Pull /var/log/auth.log or /var/log/secure for UID-switching events (su, sudo, newgrp) executed by Plesk subscriber accounts (UIDs typically in the 10000+ range in Plesk-managed environments). Capture a timestamped listing of all authorized_keys files across all home directories: 'find /var/www/vhosts /root /home -name authorized_keys -exec ls -la {} \; -exec cat {} \;'. Export the current sudoers file and all files under /etc/sudoers.d/ for comparison against baseline. MITRE ATT&CK T1548.003 (Sudo and Sudo Caching) and T1078.003 (Valid Accounts: Local Accounts) are the primary techniques to hunt for in these log sources.

Step 3: Eradication — Apply the official Plesk patch referenced in Plesk support article CVE-2025-66430 (support.plesk.com/hc/en-us/articles/36261922405015) immediately. Confirm the installed Plesk version matches the patched version specified in the advisory. Re-enable the Password Protected Directories feature only after patching is confirmed. Rotate all credentials for accounts that had access to the Plesk panel on potentially exposed servers (aligned with D3-CRO Credential Rotation and D3-CH Credential Hardening, NIST AC-2 Account Management).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST AC-2 (Account Management), NIST CM-3 (Configuration Change Control), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 5.2 (Use Unique Passwords)

Compensating: Apply the Plesk patch via CLI: 'plesk installer --select-release-current --upgrade' then verify with 'plesk version' — confirm the output matches the patched release number stated in the Plesk advisory for CVE-2025-66430. For credential rotation without a PAM or secrets manager, generate new passwords using 'openssl rand -base64 24' for each Plesk admin and reseller account, then update via 'plesk bin admin --set-admin-password -passwd '. For subscriber/client accounts: 'plesk bin client --update -passwd '. Rotate database passwords for all MySQL/PostgreSQL instances managed by Plesk by querying 'plesk db "SELECT User, Host FROM mysql.user"' and updating each credential. Document all rotations with timestamps for the post-incident record.

Evidence: Before applying the patch, preserve a forensic image or at minimum a tarball of /usr/local/psa/ (the Plesk installation directory) and /etc/sw/ to capture the vulnerable configuration state and any attacker modifications to Plesk's internal scripts or configuration files. Run 'rpm -qa | grep psa' (RHEL) or 'dpkg -l | grep psa' (Debian) to document the pre-patch Plesk package versions. After patching, re-run the same command and diff the output to confirm all Plesk components updated, not just the base package. Capture a snapshot of /var/www/vhosts/*/httpdocs/.htpasswd files — the Password Protected Directories feature writes htpasswd files here, and a malicious exploit may have injected entries or modified these files to maintain access or extract hashed credentials.

Step 4: Recovery — After patching, validate that the Plesk version string reflects the patched release. Audit all local accounts and sudo configurations on affected servers for unauthorized additions or modifications (aligned with NIST AC-6 Least Privilege, CIS 5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts, and D3-UAP User Account Permissions). Review web application and server audit logs for signs of post-exploitation activity — data exfiltration, backdoor installation, or lateral movement — going back at least 30 days (aligned with NIST AU-11 Audit Record Retention). Monitor root-level activity for 30 days post-remediation using SIEM alerting.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-6 (Least Privilege), NIST AU-11 (Audit Record Retention), NIST AC-2 (Account Management), NIST CM-6 (Configuration Settings), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Validate Plesk version with 'plesk version --full' and compare against the patched build number in the advisory. Audit local accounts by diffing the current /etc/passwd against your pre-containment baseline snapshot; flag any UIDs below 1000 added post-incident and any Plesk subscriber accounts (UID 10000+) with a shell other than /bin/false or /usr/sbin/nologin. For 30-day root monitoring without a SIEM, deploy a lightweight auditd rule: 'auditctl -a always,exit -F uid=0 -F auid!=0 -S execve -k root_escalation' and forward /var/log/audit/audit.log to a centralized syslog server daily via rsyslog. Install OSSEC or Wazuh (free) on affected servers to alert on /etc/passwd, /etc/sudoers, and authorized_keys modifications in real time.

Evidence: Search Apache/Nginx access logs at /var/log/plesk/nginx/ and /var/www/vhosts/*/logs/ for POST requests with anomalously large response bodies (potential data exfiltration) or requests to /plesk/admin endpoints from non-administrative IPs within the 30-day lookback window. Hunt for webshells in Plesk-managed document roots: 'find /var/www/vhosts -name "*.php" -newer /usr/local/psa/admin/conf/panel.ini -ls' flags PHP files created or modified after the Plesk configuration timestamp. Check for unauthorized SSH authorized_keys entries added to root's home: 'cat /root/.ssh/authorized_keys' and compare against your pre-incident baseline. Review /var/log/plesk/panel.log for API calls to backup or export functions (a post-exploitation data staging indicator) during the compromise window.

Step 5: Post-Incident — Assess whether the Password Protected Directories feature, or similar low-privilege user-facing features, were included in your last threat model review. Implement least-privilege access controls on all Plesk user accounts, limiting who can access sensitive features (NIST AC-6, CIS 5.4). Establish automated patch notification monitoring for Plesk advisories. Review your vulnerability management process to ensure hosting control panel software is included in regular patch cycles (CIS 7.1 Establish and Maintain a Vulnerability Management Process, CIS 7.3 Perform Automated Operating System Patch Management). Evaluate separation of duties for multi-tenant Plesk environments (NIST AC-5 Separation of Duties).

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST AC-6 (Least Privilege), NIST AC-5 (Separation of Duties), NIST RA-3 (Risk Assessment), NIST SI-2 (Flaw Remediation), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 7.3 (Perform Automated Operating System Patch Management)

Compensating: Subscribe to Plesk's official security advisory RSS feed (blog.plesk.com) and create a free alert via RSS-to-email tooling (e.g., Blogtrottr) so your team receives notification within hours of any new Plesk security bulletin. Enumerate Plesk user roles and permissions quarterly using 'plesk bin client --list' and 'plesk bin reseller --list', then audit which accounts have the 'Manage hosting' or 'Password Protected Directories' permission enabled and remove it where not operationally required. For multi-tenant environments, implement Plesk's Service Plan restrictions to prevent subscriber accounts from accessing the Password Protected Directories feature entirely unless explicitly granted, reducing the attack surface for any future vulnerability in that feature. Document the lessons-learned findings from this incident — specifically the gap between Plesk's release of the patch and your team's awareness — and set a patch SLA for hosting control panel software of 72 hours for CVSS ≥ 8.0.

Evidence: Produce a final incident timeline from /var/log/plesk/panel.log correlating: (1) earliest possible exploit window based on CVE-2025-66430 public disclosure date, (2) first anomalous Password Protected Directories API call, and (3) any root-level command execution events from auditd — this timeline is the primary deliverable for the post-incident report and any regulatory notification assessment. Archive all collected log files, the pre-patch /usr/local/psa/ tarball, the pre- and post-patch package version diffs, and the authorized_keys and sudoers baselines to a write-protected evidence repository (external S3 bucket with object lock, or an offline encrypted drive) before closing the incident.

Detection Guidance

Query system-level logs (auth.log, /var/log/secure, auditd logs) on Plesk-managed servers for privilege escalation events, specifically transitions to root from accounts associated with the Plesk service (psaadm, apache, or tenant-level accounts). Look for execve() syscalls or shell invocations (bash, sh, perl, python) triggered by Plesk process trees outside expected administrative operations. Check for modifications to /etc/passwd, /etc/sudoers, /etc/sudoers.d/, and authorized_keys files under root or high-privilege accounts (D3-SFA System File Analysis). Alert on new cron entries added under /var/spool/cron/root or /etc/cron.d/ by non-root processes. In SIEM, correlate Plesk web panel access logs (typically /var/log/plesk/panel.log and /usr/local/psa/var/log/) with subsequent root-level OS activity within short time windows. No public IOCs (IP, domain, hash) are associated with active exploitation of this CVE at this time. The EPSS score (0.043%, 13th percentile) suggests limited observed in-the-wild exploitation, but absence of IOCs does not confirm absence of targeting. Align detection with NIST SI-4 System Monitoring and AU-6 Audit Record Review.

Framework Mappings

MITRE-ATTACK

- **T1059** — Command and Scripting Interpreter
- **T1068** — Exploitation for Privilege Escalation

NIST-800-53R5

- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring

- **SI-7** — Software, Firmware, and Information Integrity
- **AC-6** — Least Privilege
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-10** — Information Input Validation

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control
- **A03:2021** — Injection

CIS-V8

- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts
- **6.8** — Define and Maintain Role-Based Access Control
- **2.5** — Allowlist Authorized Software
- **16.10** — Apply Secure Design Principles in Application Architectures
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

SOC2-TSC

- **CC6.3** — Authorizes, modifies, or removes access

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1059	Command and Scripting Interpreter	Execution
T1068	Exploitation for Privilege Escalation	Privilege-Escalation

Sources

Source	URL	Tier
	https://gbhackers.com/critical-plesk-vulnerability/	T3
Critical Plesk Vulnerability Let Users Execute Arbitrary Commands ...	https://x.com/f1tym1/status/2061426209905344742	T3
[CVE-2025-66430] Security vulnerability in Password Protected ...	https://support.plesk.com/hc/en-us/articles/36261922405015--CVE-202...	T3

Source	URL	Tier
Critical Plesk Vulnerability Allows Plesk Users to Gain Root-Level ...	https://community.opentextcybersecurity.com/vulnerability-vault-228...	T3
Warning: Privilege Escalation in Plesk, Patch Immediately!	https://ccb.belgium.be/advisories/warning-privilege-escalation-ples...	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2025-66430	T1

Generated 2026-06-01 13:38 UTC by TJS Security Command Center