Nro. Alerta:	AL-2026-025	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DE ARCOTEL **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	4-may-2026	Falla crítica en cPanel/WHM permite acceso root sin autenticación (CVE-2026-41940)	Pág.: **1** of **7**

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de Incidente: Bypass de autenticación y escalada de privilegios remota
Nivel de riesgo: Alta

II. ALERTA

Figura 1.- Falla crítica en cPanel/WHM permite acceso root sin autenticación (CVE-2026-41940) - figura referencial

cPanel reveló una vulnerabilidad crítica 0-day de omisión de autenticación (authentication bypass) registrada como CVE-2026-41940. El fallo corresponde a un ataque de manipulación de archivos de sesión mediante inyección CRLF (Carriage Return y Line Feed), en el cual un atacante no autenticado inserta líneas especialmente diseñadas dentro de un archivo de sesión antes del proceso de autenticación. Como resultado, el sistema interpreta estos datos manipulados como válidos, permitiendo al atacante obtener acceso a nivel de root en la interfaz administrativa de WHM (Web Host Manager), sin necesidad de credenciales válidas.

III. INTRODUCCIÓN

cPanel es un popular panel de administración utilizado en decenas de millones de dominios, que permite gestionar de forma gráfica un servidor o una cuenta de hosting sin necesidad de usar comandos de Linux. La compañía alertó a su comunidad sobre la vulnerabilidad crítica CVE-2026-41940, de tipo pre-autenticación en:

- CPanel, que es el panel destinado a usuarios finales, utilizado para administrar sitios web, configuraciones de correo electrónico y dominios, bases de datos y transferencia de archivos.
- WHM (Web Host Manager) es la interfaz de administración de cPanel a nivel del servidor, utilizada por administradores o proveedores de hosting.

La vulnerabilidad permite que un atacante remoto no autenticado pueda escalar privilegios a ROOT dentro de la interfaz de WHM, explotando la combinación de dos debilidades:

- **Inyección CRLF** en el procesamiento de autenticación HTTP Basic, lo que permite a un atacante no autenticado inyectar pares de clave-valor empleando los caracteres CR (**\r**) y LF (**\n**) en un archivo de inicio de sesión arbitraria en el almacén de sesiones del lado del servidor antes de la autenticación, por ejemplo, el sistema espera.

  Entrada del sistema: user=name
  El atacante inyecta: user**\r\n**rol=admin
  El servidor interpreta la entrada como:
  user=name
  rol=admin

- **Condición de carrera (race condition)** en el almacenamiento dual de sesiones: cPanel guarda los datos de sesión tanto en un archivo de texto como en una caché JSON. Los datos inyectados pueden persistir durante esta ventana de inconsistencia y la capa de autenticación termina confiando en ellos.

Posteriormente, cuando se ejecuta el proceso cpsrvd (el daemon de cPanel), este vuelve a analizar el archivo de sesión. En ese momento, las líneas previamente inyectadas se interpretan como entradas válidas de sesión de alto nivel, incluyendo valores como user=root, hasroot=1, tfa_verified=1, un cp_security_token controlado y un

nuevo successful_internal_auth_with_timestamp. Estos valores provocan que la sesión sea elevada a una sesión completamente autenticada como **root**, omitiendo tanto la verificación de contraseña como el mecanismo de segundo factor de autenticación (2FA), sin que se ejecute el flujo normal de autenticación del sistema

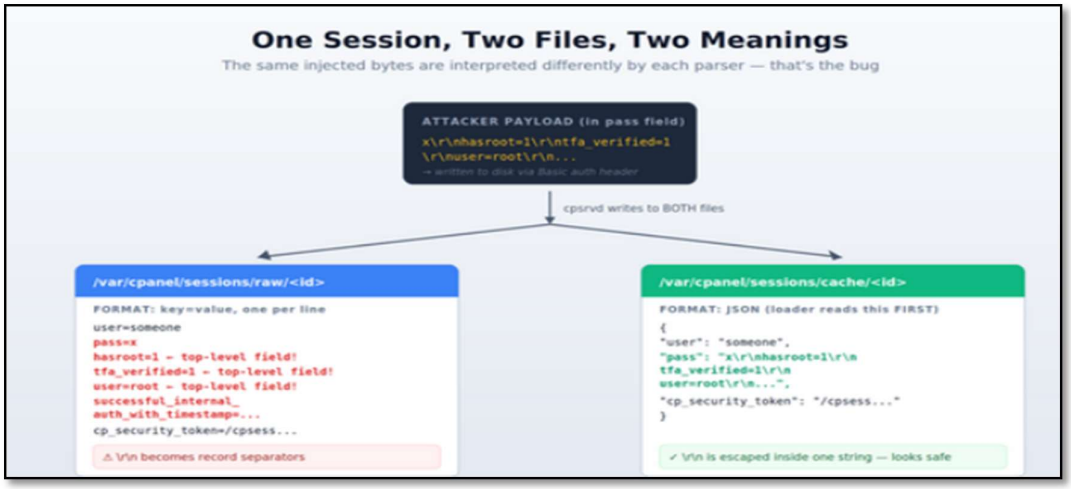

Figura 2.- Diagrama de inyección CRLF de archivo de sesión de cPanel frente a caché JSON CVE-2026-41940

IV. VECTOR DE ATAQUE

El vector es de tipo RED, CVSS:3.1/AV: N/AC: L/PR: N/UI: N/S: U/C:H/I:H/A:H con una puntuación de 9.8.

Se detalla el proceso de ataque:

Figura 3.- Explotación de CVE-2026-41940 en cuatro pasos para el acceso root.

1. **Falla de inicio de sesión**:

El atacante falla un inicio de sesión (por ejemplo, POST /login/?login_only=1 con user=root&pass=wrong) para crear un archivo de sesión previo a la autenticación. La respuesta del servidor establece una cookie de sesión de whostmgression que contiene un id de sesión aleatoria y un sufijo de ofuscación.

2. **Inyección CRLF a través de HTTP Basic auth:**

El atacante reutiliza la cookie sin el sufijo de ofuscación y envía una cabecera Authorization: Basic, donde el contenido decodificado contiene, en texto plano (raw) la inyección CRLF:

root:x**\r\n**hasroot=1**\r\n**tfa_verified=1**\r\n**user=root**\r\n**cp_security_token=/cpsess99999999**\r\n**successful_inthernal_auth_with_timestamp=**\r\n.**

Luego saveSession() escribe la contraseña (con saltos de línea incrustados) tal cual en /var/cpanel/sessions/raw/. El archivo ahora contiene registros de múltiples líneas en formato clave=valor.

3. **Disparador de regeneración de la cache**:

El atacante solicita una URL protegida con el prefijo de token elegido (GET /cpsess9999999999/scripts2/listaccts). La caché aún no ha sido regenerada, por lo que el token asociado a la URL no coincide, se activa do_token_denied(), y Modify::new(nocache => 1) vuelve a analizar el archivo raw que ahora contiene múltiples líneas.

El módulo RModify::save() reescribe la caché JSON con cada clave analizada, incluyendo la del atacante, promovida a una entrada de sesión de nivel superior, llevando a cabo la inyección de privilegios, la sesión ahora se interpreta como:

user=root, hasroot=1, tfa_verified=1, cp_security_token=/cpsess9999999999, successful_internal_auth_with_timestamp=….

4. **Solicitud autenticada como root:**

Una solicitud GET posterior a /cpsess9999999999/ pasa la verificación del token en la URL, la marca de tiempo de autenticación reciente suprime la validación de la contraseña y tfa_verified=1 suprime la validación del doble factor de seguridad.

cpsrvd ejecuta el manejador como root. GET /cpsess9999999999/json-api/ version?api.version=1 es la prueba mínima inequívoca — devuelve un documento JSON que contiene la versión de compilación de cPanel, ejecutado con privilegios de root.

V. IMPACTO

Campo	Detalle
Producto afectado	cPanel y WHM
Versiones afectadas	Todas las versiones compatibles posteriores a 11.40
Superficie de exposición	Servicios accesibles a través de Internet
Puertos asociados	2087 (WHM) / 2083 (cPanel)
Nivel de riesgo	Alto en sistemas con acceso público
Condición de explotación	Servicios expuestos sin restricciones de acceso

Tabla 1.- Sistemas afectados - Falla crítica en cPanel/WHM permite acceso root sin autenticación (CVE-2026-41940)

VI. INDICADORES DE COMPROMISO

Categoría	Indicador	Descripción
Filesystem	Presencia de \r\n en valores de sesión	Inserción de saltos de línea en archivos /var/cpanel/sessions/raw/
Filesystem	grep -P 'pass=.*\r' /var/cpanel/sessions/raw/*	Búsqueda de valores manipulados en sesiones
Sesiones	hasroot=1	Indica elevación de privilegios en sesión
Sesiones	successful_internal_auth_with_timestamp	Marca de autenticación interna manipulada
Sesiones	tfa_verified=1	Posible bypass de autenticación multifactor
Logs	Código 307 redirect sin login previo	Redirección sospechosa sin autenticación válida
Logs	cpsessXXXXXXXXXX sin POST /login/	Indica autenticación forzada
Logs	/usr/local/cpanel/logs/access_log	Archivo a revisar para actividad sospechosa
Cookies	Cookie whostmgrsession truncada	Sesión manipulada sin sufijo válido
Cookies	Header Authorization: Basic	Uso de autenticación básica para inyección
SIEM	Coincidencia Cookie + Authorization: Basic	Patrón de detección en logs/SIEM

Tabla 5.- Indicadores Asociados - Falla crítica en cPanel/WHM permite acceso root sin autenticación (CVE-2026-41940)

VII. RECOMENDACIONES:

- Aplicar de inmediato las actualizaciones de seguridad publicadas por cPanel para mitigar la vulnerabilidad CVE-2026-41940.
- Restringir el acceso a los puertos 2083 y 2087 mediante firewall, VPN o listas de control de acceso, evitando su exposición directa a Internet.
- Revisar los archivos de sesión (/var/cpanel/sessions/raw/) en busca de patrones anómalos como \r\n, hasroot=1 o tfa_verified=1.
- Analizar los registros en /usr/local/cpanel/logs/access_log para detectar redirecciones 307 sin autenticación previa o accesos sospechosos con cpsess.
- Monitorear el uso de cabeceras Authorization: Basic junto con cookies de sesión, como posible indicador de explotación.
- Rotar credenciales administrativas y revisar configuraciones, cuentas y claves SSH ante posibles indicios de compromiso.
- En caso de actividad sospechosa, aislar el sistema afectado y realizar un análisis forense.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

CSIRT TELCONET (2026). *Vulnerabilidad de bypass de autenticación en cPanel y WHM*. https://csirt.telconet.net/comunicacion/boletines-servicios/vulnerabilidad-critica-de-bypass-de-autenticacion-en-cpanel-y-whm/

CPANEL (2026). *Security Advisory: CVE-2026-41940 cPanel & WHM / WP2 Security Update*. https://support.cpanel.net/hc/en-us/articles/40073787579671-Security-CVE-2026-41940-cPanel-WHM-WP2-Security-Update-04-28-2026

TREND MICRO (2026). *Critical Authentication Bypass in cPanel & WHM (CVE-2026-41940)*. https://success.trendmicro.com/en-US/solution/KA-0023294

PICUS SECURITY (2026). *CVE-2026-41940 explained: cPanel & WHM authentication bypass*. https://www.picussecurity.com/resource/blog/cve-2026-41940-explained-cpanel-whm-authentication-bypass-hit-1-5m-servers

MITRE (2026). *CVE-2026-41940*. https://www.cve.org/CVERecord?id=CVE-2026-41940