I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de Incidente: Despliegue de Ransomware
Nivel de riesgo: Alta

II. ALERTA

Figura 1.- Explotación activa de CVE-2026-41940 permite despliegue del Ransomware Sorry en cPanel/WHM - figura referencial

Tras la explotación activa de la vulnerabilidad 0-day CVE-2026-41940 en cPanel/WHM que permite a un atacante remoto no autenticado escalar privilegios desde una sesión de cPanel hasta WHM como root y obtener control total del servidor, la plataforma vuelve a captar la atención de los equipos de ciberseguridad, luego de que actores maliciosos comenzaran a explotarla para desplegar el Ransomware "Sorry".

III. INTRODUCCIÓN

La explotación de la vulnerabilidad CVE-2026-41940 fue la parte inicial de una campaña activa por parte de los atacantes, puesto que aprovecharon el acceso obtenido a través de los paneles cPanel/WHM comprometidos para desplegar un Ransomware llamado Sorry desarrollado en Go y orientado específicamente a sistemas Linux.

Usuarios reportaron que sus sitios web se han visto afectados por los ataques, dejando rastros visibles en buscadores, varios de los sitios comprometidos quedaron indexados por Google mostrando mensajes asociados al grupo de atacantes.

El malware añade la extensión **.sorry** a los archivos afectados y genera una nota de rescate llamada README.md en cada carpeta, estas notas de rescate incluían un identificador de contacto en la red Tox (el protocolo de mensajería encriptado difícil de rastrear), para negociar pagos con las víctimas. El mismo ID apareció repetido en los distintos incidentes reportados.

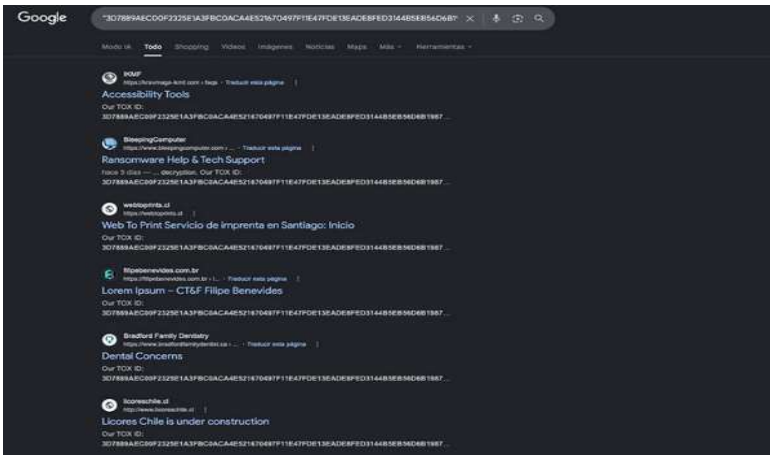

Figura 2.- Sitios encriptados por Sorry e indexados en Google - Explotación activa de CVE-2026-41940 permite despliegue del Ransomware Sorry en cPanel/WHM

Figura 3.- Nota de rescate - Explotación activa de CVE-2026-41940 permite despliegue del Ransomware Sorry en cPanel/WHM

En el 2018, una campaña del Ransomware Sorry utilizó un cifrador HiddenTear para cifrar archivos y agregar la extensión .sorry a los archivos de sus víctimas, pero esta campaña actual utiliza un cifrador diferente y no está relacionada con la anterior.

Los especialistas señalaron que el Ransomware Sorry utiliza el cifrado Cha-Cha20 para bloquear archivos, mientras que la clave de cifrado quedó protegida mediante una clave pública RSA-2048 incrustada en el malware.

IV. VECTOR DE ATAQUE

La vulnerabilidad CVE-2026-41940 posee un vector de ataque de tipo RED CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H con nivel de severidad 9.8 CRÍTICO.

T1190 - Explotación de una aplicación expuesta públicamente el principal despliegue del Ransomware Sorry se centra en el acceso inicial de servidores ya comprometidos o nuevas explotaciones mediante Inyección CRLF en el procesamiento de autenticación HTTP Basic de la vulnerabilidad CVE-2026-41940, 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.

Figura 4.- Cadena de ataque por inyección CRLF - Explotación activa de CVE-2026-41940 permite despliegue del Ransomware Sorry en cPanel/WHM

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 - Explotación activa de CVE-2026-41940 permite despliegue del Ransomware Sorry en cPanel/WHM

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 2.- Indicadores Asociados - Explotación activa de CVE-2026-41940 permite despliegue del Ransomware Sorry en cPanel/WHM

VII. RECOMENDACIONES:

- Una medida de contención efectiva es limitar o cerrar los puertos de cpsrvd mediante lista blanca hacia IPs de administración, en particular 2082, 2083, 2086, 2087, 2095 y 2096.
- También se recomienda situar cpsrvd detrás de un punto de inspección, por ejemplo Apache con ModSecurity y exponer el acceso mediante proxy subdomains, dejando los puertos directos inaccesibles desde Internet.
- Añadir reglas WAF para bloquear CR o LF tras decodificar Authorization Basic y para rechazar cookies whostmgrsession con formato anómalo.
- Ejecutar un escaneo forense de sesiones en /var/cpanel/sessions/raw y correlacionarlo con logs de acceso y login, buscando combinaciones sospechosas como token_denied junto con cp_security_token y origin_as_string con method=badpass.

- Tras actualizar, purgar sesiones potencialmente manipuladas y reiniciar el servicio cpsrvd para reducir el riesgo de reutilización de artefactos antiguos.
- Comprobar si las actualizaciones están deshabilitadas o fijadas a una versión, por ejemplo, mediante /etc/cpupdate.conf y corregirlo para permitir parches de emergencia.

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:

BLEEPINGCOMPUTER (2026). *Critrical cPanel flaw mass-exploited in "Sorry" ransomware attacks*. https://www.bleepingcomputer.com/news/security/critrical-cpanel-flaw-mass-exploited-in-sorry-ransomware-attacks/

ECUCERT (2026). *AI-2026-025: Falla crítica en cPanel/WHM permite acceso root sin autenticación (CVE-2026-41940)*.https://www.ecucert.gob.ec/wpcontent/uploads/2026/05/AI-2026-025-Falla-critica-en-cPanel-WHM-permite-acceso-root-sin-autenticacion-CVE-2026-41940.pdf

CENTER FOR INTERNET SECURITY – CIS (2026). *A Vulnerability in WHM/cPanel and WP Squared Could Allow for Remote Code Execution*. https://www.cisecurity.org/advisory/a-vulnerability-in-whm-cpanel-and-wp-squared-could-allow-for-remote-code-execution_2026-042

HELP NET SECURITY (2026). *Multiple threat actors actively exploit cPanel vulnerability CVE-2026-41940*. https://www.helpnetsecurity.com/2026/05/04/multiple-threat-actors-actively-exploit-cpanel-vulnerability-cve-2026-41940/

OHMYGEEK (2026). *Falla crítica en cPanel CVE-2026-41940*. https://ohmygeek.net/2026/05/04/falla-cpanel-cve-2026-41940/

HISPASEC – UNA AL DÍA (2026). *Explotación masiva de un bypass crítico en cPanel facilita el ransomware Sorry en servidores Linux*. https://unaaldia.hispasec.com/2026/05/explotacion-masiva-de-un-bypass-critico-en-cpanel-facilita-el-ransomware-sorry-en-servidores-linux.html

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/