CVE-2026-53997: Account Takeover mediante endpoint de activación sin autenticación en Netherman

Investigación y divulgación responsable · Netherman / portaldelhermano.es · 2026

CVE-2026-53997 | CVSS 7.4 HIGH | Account Takeover | Broken Authentication | Missing Rate Limiting

Resumen

Esta investigación documenta una vulnerabilidad de **account takeover completo sin autenticación** en la plataforma SaaS **portaldelhermano.es**, desarrollada por **Netherman** y utilizada por más de **80 hermandades** en toda España. El endpoint /password/create-access expone cuatro comprobaciones de verificación secuenciales —DNI, fecha de nacimiento, teléfono e IBAN (últimos 4 dígitos)— sin ningún tipo de limitación de tasa, bloqueo por IP ni control de intentos, lo que permite a un atacante remoto obtener acceso total a cualquier cuenta sin credenciales.
Los datos expuestos tras el compromiso incluyen DNI completo, IBAN, teléfono, fecha de nacimiento y documentos fiscales (Modelo 182). El CVE fue asignado por **VulnCheck** con identificador **CVE-2026-53997** y puntuación **CVSS 7.4 HIGH**.

Descripción de la plataforma

Netherman es una plataforma de gestión para hermandades y cofradías, accesible a través de portaldelhermano.es. Centraliza información de hermanos, cuotas, datos bancarios y documentos fiscales. Su uso está extendido entre hermandades de distintas comunidades autónomas, lo que implica que los datos de miles de personas están alojados en una única infraestructura compartida.

Análisis técnico

El flujo de restablecimiento de acceso de la plataforma se articula en torno al endpoint POST /password/create-access. Este endpoint implementa un proceso de verificación de identidad en cuatro pasos secuenciales, en el que cada paso actúa como una comprobación independiente:

Paso 1 · DNI: Se solicita el número de DNI del hermano. La respuesta del servidor difiere según si el DNI existe o no en la base de datos, exponiendo una **respuesta diferencial que permite enumerar DNIs válidos**.

Paso 2 · Fecha de nacimiento: Una vez identificado el DNI, se solicita la fecha de nacimiento. Al estar acotada por la lógica de negocio de la plataforma (rango de fechas plausible para un hermano activo), el espacio de búsqueda se reduce a aproximadamente **21.900 peticiones**, completables en ~2 minutos sin ningún bloqueo.

Paso 3 · Teléfono: Se solicita el número de teléfono del hermano. Recuperable mediante técnicas de OSINT (redes sociales, directorios públicos, webs de hermandades).

Paso 4 · IBAN (últimos 4 dígitos): El último factor son los 4 últimos dígitos del IBAN. Con un espacio de búsqueda de **~10.000 combinaciones** y sin limitación de intentos, la fuerza bruta es trivial.

Ninguno de los cuatro pasos implementa **rate limiting**, **CAPTCHA**, **bloqueo por IP** ni **límite de intentos**. La cadena completa puede automatizarse y ejecutarse de forma remota, sin acceso físico ni credenciales previas.

Impacto

Un atacante que complete la cadena obtiene control total sobre la cuenta del hermano. Los datos accesibles tras el compromiso incluyen:

- DNI completo
- IBAN completo
- Número de teléfono
- Fecha de nacimiento
- Documentos fiscales (**Modelo 182**)
- Historial de pagos y cuotas

La exposición afecta a **todos los hermanos registrados en la plataforma**, distribuidos entre más de 80 hermandades en España. Se trata de datos especialmente sensibles desde el punto de vista del RGPD: identificación personal, datos bancarios y documentos tributarios.

Vector CVSS 3.1

AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N — **CVSS 7.4 HIGH**

AV:N — Explotable de forma remota, sin acceso físico
AC:H — Complejidad alta (requiere OSINT previo para el teléfono)
PR:N — Sin privilegios previos
UI:N — Sin interacción del usuario
C:H / I:H — Confidencialidad e integridad totalmente comprometidas
A:N — Sin impacto en disponibilidad

Línea de tiempo

14 jun. 2026 Descubrimiento de la vulnerabilidad durante investigación de seguridad.

14 jun. 2026 Reporte enviado a **VulnCheck** mediante proceso de divulgación responsable.

22 jun. 2026 VulnCheck confirma la recepción del reporte y asigna el identificador **CVE-2026-53997**. Plazo de divulgación: 20 de octubre de 2026.

6 oct. 2026 Se verifica que el proveedor ha corregido la vulnerabilidad de forma silenciosa, sin publicar ningún aviso público ni agradecimiento formal.

12 oct. 2026 Publicación de este advisory como referencia pública, necesaria para proceder con la emisión del CVE.

Recomendaciones

- Implementar **rate limiting** estricto en todos los endpoints de verificación de identidad (máximo 5 intentos por IP y bloqueo progresivo).
- Añadir **CAPTCHA** o mecanismo anti-bot tras el primer intento fallido.
- Sustituir el modelo de verificación en múltiples pasos secuenciales por un flujo fuera de banda (envío de código por SMS o email).
- Implementar **alertas de seguridad** que notifiquen al usuario cuando se inicia un proceso de recuperación de acceso en su cuenta.
- Auditar los logs de acceso al endpoint /password/create-access para detectar patrones de abuso previos.

Referencias

CVE-2026-53997 — CVE.org

VulnCheck Advisory — Netherman Portal del Hermano Account Takeover via Password Reset Oracle

© 2026 Beatriz Fresno Naumova — beafn28.es. Todos los derechos reservados.

Política de privacidad · Términos de uso · Política de cookies