Boletín de alerta

Boletín Nro.: 57
Fecha de publicación: 11/07/2025
Tema: Alerta 2025-57 Vulnerabilidades importantes en Ivanti
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

- Endpoint Manager Mobile (EPMM)
  - 12.5.0.1 y anteriores
  - 12.4.0.2 y anteriores
  - 12.3.0.2 y anteriores
- Endpoint Manager EPM 2022 SU8 and EPM 2024 SU2
  - 2022 SU8 y anteriores
  - 2024 SU2 y anteriores

Descripción

Se ha reportado varias vulnerabilidades en productos Ivanti, de entre ellas podemos destacar CVE-2025-6995 (CVSS 8.4) y CVE-2025-6996 (CVSS 8.4) ambas relacionadas al uso indebido del cifrado en el agente de Ivanti Endpoint Manager EMP.

A continuación se listan las vulnerabilidades detectadas para EPM:

- El CVE-2025-6995 y CVE-2025-6996 se relacionan con el uso indebido del cifrado en el agente de Ivanti Endpoint Manager anterior a la versión 2024 SU3 y 2022 SU8 Security Update 1 permite que un atacante local autenticado descifre las contraseñas de otros usuarios.
- CVE-2025-7037 (CVSS 7.2): La inyección de SQL en Ivanti Endpoint Manager anterior a la versión 2024 SU3 y 2022 SU8 Security Update 1 permite que un atacante remoto autenticado con privilegios de administrador lea datos arbitrarios de la base de datos.

También podemos destecar dos vulnerabilidades en el producto Ivanti Endpoint Manager Mobile (EPMM), CVE-2025-6770 (CVSS 7.2) y CVE-2025-6771 (CVSS 7.2) ambas son inyecciónes de comandos del sistema operativo en EPMM anterior a la versión 12.5.0.2 permite que un atacante remoto autenticado con altos privilegios logre la ejecución remota de código.

Solución:

Se recomienda aplicar los parches publicados por el fabricante:

- Ivanti Endpoint Manager Móvil:
  - Versiones resueltas:
    - 12.5.0.2
    - 12.4.0.3
    - 12.3.0.3
  - Portal de descarga: **https://portal.ivanti.com/**
- EMP
  - Versiones resueltas:
    - Actualización de seguridad SU8 2022 1
    - 2024 SU3
  - Portal de descarga: https://forums.ivanti.com/s/article/How-to-access-software-downloads-in-the-Ivanti-License-System

Información adicional:

- https://forums.ivanti.com/s/article/Security-Advisory-July-2025-for-Ivanti-EPM-2024-SU2-and-EPM-2022-SU8?language=en_US&_gl=1*1v71q4t*_gcl_au*MjA5NzkwNzU5OS4xNzUyMjU5ODE3
- https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2025-6770-CVE-2025-6771?language=en_US&_gl=1*1v71q4t*_gcl_au*MjA5NzkwNzU5OS4xNzUyMjU5ODE3
- **https://www.ivanti.com/blog/july-security-update-2025**