Veeam ha lanzado actualizaciones de seguridad para corregir un total de 18 vulnerabilidades en sus productos de software, entre las que se incluyen cinco fallos críticos que podrían permitir la ejecución remota de código.

La lista de vulnerabilidades es la siguiente:

- CVE-2024-40711 (Puntuación CVSS: 9.8): Un fallo en Veeam Backup & Replication que posibilita la ejecución de código remoto sin necesidad de autenticación.
- CVE-2024-42024 (Puntuación CVSS: 9.1): Un fallo en Veeam ONE que permite a un atacante con acceso a las credenciales de la cuenta del servicio Agente ejecutar código remoto en la máquina afectada.
- CVE-2024-42019 (Puntuación CVSS: 9.0): Un fallo en Veeam ONE que permite a un atacante obtener el hash NTLM de la cuenta de servicio de Veeam Reporter Service.
- CVE-2024-38650 (Puntuación CVSS: 9.9): Una vulnerabilidad en Veeam Service Provider Console (VPSC) que concede a un atacante con pocos privilegios acceso al hash NTLM de la cuenta de servicio en el servidor.
- CVE-2024-39714 (Puntuación CVSS: 9.9): Un fallo en VPSC que permite a un usuario con permisos limitados subir archivos arbitrarios al servidor, resultando en la ejecución remota de código en el mismo.

Además, las actualizaciones de septiembre de 2024 también resuelven otras 13 vulnerabilidades graves que podrían permitir la escalada de privilegios, la elusión de la autenticación multifactor (MFA) y la ejecución de código con privilegios elevados.

Las versiones donde se han corregido estos problemas son las siguientes:

- Veeam Backup & Replication 12.2 (versión 12.2.0.334)
- Veeam Agent para Linux 6.2 (versión 6.2.0.101)
- Veeam ONE v12.2 (versión 12.2.0.4093)
- Veeam Service Provider Console v8.1 (versión 8.1.0.21377)
- Veeam Backup para Nutanix AHV Plug-In v12.6.0.632
- Veeam Backup para Oracle Linux Virtualization Manager y Red Hat Virtualization Plug-

In v12.5.0.299

Dado que estas fallas en el software de Veeam están atrayendo la atención de actores maliciosos interesados en distribuir ransomware, se aconseja a los usuarios actualizar a la versión más reciente lo antes posible para evitar posibles amenazas.