BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-15
Fecha de publicación: 11/06/2024
Tema: Vulnerabilidad critica en Veeam Backup con exploit público.
Traffic Light Protocol (TLP): White

Producto(s) afectado:

Veeam Backup Enterprise Manager

- Versiones afectadas:
  - Anterior a la 12.1.2.172

Descripción

El 21 de mayo del 2024, Veeam alertó que se descubrió una falla de seguridad en el software de Veeam Backup Enterprise Manager denominada como CVE-2024-29849, con una puntuación de severidad de 9.8 (Alta).

Esta vulnerabilidad consiste en la omisión de autenticación, que permitiría a un atacante manipular los respaldos de nuestra la infraestructura, esto resulta importante porque, un atacante al infiltrarse en la red podría utilizar esta vulnerabilidad a su conveniencia para, una vez dentro de la red, impactar las copias de seguridad. Esta técnica es muy utilizada por grupos de ransomware quienes, antes de cifrar los archivos, buscan llegar a los backups y destruirlos.

Recientemente se publicó un exploit como prueba de concepto de esta vulnerabilidad, lo que aumenta por mucho la probabilidad de explotación de esta, en entornos empresariales lo que podría llevar a un gran daño a la producción si es que los respaldos internos también se ven afectados.

Impacto

Un actor malintencionado que pueda estar internamente en la red, podría aprovechar esta vulnerabilidad para borrar parcial o totalmente las copias de seguridad, con lo que no se podría regresar a un respaldo para recuperar el funcionamiento.

Solución

Actualizar el software Veeam Backup Enterprise Manager a la versión 12.1.2.172 o posterior.

Información adicional:

- https://securityaffairs.com/164407/hacking/veeam-cve-2024-29849-poc.html
- https://www.veeam.com/kb4581
- https://securityboulevard.com/2024/06/cve-2024-29849-veeam-discloses-critical-vulnerability-that-allows-attackers-to-bypass-user-authentication-on-its-backup-enterprise-manager-web-interface/
- https://summoning.team/blog/veeam-enterprise-manager-cve-2024-29849-auth-bypass/

BEACON LAB

C S I R T

CYBOLT

Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com