



## **BOLETÍN DE ALERTA**

**Boletín Nro.:** 2023-11

**Fecha de publicación:** 24/03/2023

**Tema:** Vulnerabilidad de acceso no autorizado en productos Veeam.

### **Software afectado:**

- Veeam Backup & Replication, versiones anteriores a 12 (build 12.0.0.1420 P20230223)
- Veeam Backup & Replication, versiones anteriores a 11a (build 11.0.1.1261 P20230227)

### **Descripción:**

Se ha reportado un nuevo aviso de seguridad sobre una vulnerabilidad que afecta a productos Veeam, que permitiría a un atacante no autenticado obtener acceso al sistema afectado. Actualmente para esta vulnerabilidad existe una prueba de concepto (*PoC*) pública.

La vulnerabilidad identificada como [CVE-2023-27532](#), de severidad “Alta” y con puntuación de 7.5. Esta vulnerabilidad se debe a una falla en el control de acceso a las credenciales cifradas alojadas en la base de datos de configuración de los componentes Veeam Backup & Replication de Veeam. Un atacante no autenticado con acceso al servicio de *Backup* de Veeam (puerto *TCP* 9401 por defecto), podría solicitar credenciales almacenadas en la base de datos y tener acceso a las mismas en texto claro.

### **Impacto:**

La explotación exitosa de esta vulnerabilidad permitiría a un atacante no autenticado obtener acceso a datos confidenciales de la base de datos, como credenciales de acceso y utilizarlas para acceder al sistema afectado.

### **Solución:**

Recomendamos instalar las actualizaciones correspondientes provistas por el fabricante, mediante en los siguientes enlaces:

- [Veeam Backup & Replication 12](#)
- [Veeam Backup & Replication 11](#)

---

### **Ciberseguridad y Protección de la Información**

Ministerio de Tecnologías de la Información y Comunicación (MITIC)

Gral. Santos y Concordia - Complejo Santos - Offic. E14

[cert@cert.gov.py](mailto:cert@cert.gov.py) | +595 21 217 9000

Asunción - Paraguay | [www.cert.gov.py](http://www.cert.gov.py)





**Información adicional:**

- <https://www.horizon3.ai/veeam-backup-and-replication-cve-2023-27532-deep-dive/>
- <https://nvd.nist.gov/vuln/detail/CVE-2023-27532>
- <https://www.veeam.com/kb4424>
- <https://www.veeam.com/kb4420?ad=in-text-link>
- <https://www.veeam.com/kb4245?ad=in-text-link>

---

**Ciberseguridad y Protección de la Información**

Ministerio de Tecnologías de la Información y Comunicación (MITIC)

Gral. Santos y Concordia - Complejo Santos - Offic. E14

[cert@cert.gov.py](mailto:cert@cert.gov.py) | +595 21 217 9000

Asunción - Paraguay | [www.cert.gov.py](http://www.cert.gov.py)

