Data/VM Backups (version 1.0)

**Cloud Service Label: IaaS**

Description

Permissions to create snapshots of VM’s differ from permissions for accessing VM ephemeral storage or permissions or for accessing storage locations of backups. Even It is plausible that an adversary could create a snapshot of a VM in a directory he controls or have permissions to read a storage location where snapshots are stored and then restore the image. An adversary This could allow the adversary to gain access to any data stored within the ephemeral storage of the VM without explicit permissions.

Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
|  |  |

Mitigations

|  |  |
| --- | --- |
| **Mitigation** | **Description** |
| Ensure permissions for snapshots are managed adequately | In Azure the VM Contributor role has the right to create snapshot and a storage reader can access existing snapshots already created. |

Detection

Closely monitor API access to storage accounts associated with backups.

References

1. https://docs.microsoft.com/en-us/azure/backup/backup-rbac-rs-vault -Accessed June 17,2020