**Hamza Ghariani 4 NIDS 1 [ Workshop #3 ]**

**CVE-2021-21974**

1. **Introduction:**

**CVE-2021-21974** is a **security vulnerability** that **affects VMware's vCenter Server**, a centralized management utility for vSphere virtualization platform. The vulnerability **allows an attacker with network access** to the **vCenter Server management interface** to **execute arbitrary code** on the **underlying operating system that hosts vCenter Server**.

1. **Details:**

The vulnerability exists due to **a flaw in the vSphere Client (HTML5)** that allows an attacker to **send a specially crafted request to the vCenter Server**. This can be **exploited to execute arbitrary code on the underlying operating system**.

1. **Impact:**

This vulnerability **can be exploited remotely by an attacker** with network access to the vCenter Server management interface. Successful exploitation of this vulnerability **could lead to arbitrary code execution** on the underlying operating system. This could allow an attacker to gain **full control of the vCenter Server** and **potentially compromise the entire virtualization environment.**

1. **Solution:**

VMware released **a patch** for this vulnerability on **February 23, 2021**. It is strongly recommended that vCenter Server users apply the patch as soon as possible to prevent any potential exploitation of the vulnerability.