# Advisory Alert

**Alert Number:** AAA20210608 **Date:** June 8, 2021

**Document Classification Level :** Public Circulation Permitted | Public

**Information Classification Level :** TLP: WHITE

## Overview

| Product | Severity | Vulnerability |
|---|---|---|
| **VMware** | Critical | Multiple Vulnerabilities |
| **IBM** | **Medium** | Directory Traversal vulnerability |

## Description

| | |
|---|---|
| Affected Product | **VMware** |
| Severity | Critical – Initial advisory alert AAA20210528 release date was in 28th of May 2021, it is again added as a reminder and the update is sent as there are exploitation attempts of this vulnerability in the world. |
| Affected Vulnerability | Remote code execution (CVE-2021-21985, CVE-2021-21986) |
| Description | The vSphere Client (HTML5) Virtual SAN Health Testing Plugin contains remote code execution victim due to invalidation of input which is basically enabled in the vCenter server. A malicious actor with network access to port 443 may exploit this issue to execute commands with unrestricted privileges on the underlying operating system that hosts vCenter Server. VMware highly recommends to apply relevant patches at earliest to avoid issues. |
| Affected Products | VMware vCenter Server (vCenter Server) |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.vmware.com/security/advisories/VMSA-2021-0010.html |

| | |
|---|---|
| Affected Product | **IBM** |
| Severity | **Medium** |
| Affected Vulnerability | Directory Traversal vulnerability (CVE-2021-20517) |
| Description | IBM WebSphere Application Server Network Deployment could allow a remote authenticated attacker to traverse directories. An attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to read and delete arbitrary files on the system. |
| Affected Products | WebSphere Application Server ND<br>WebSphere Application Server ND |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.ibm.com/support/pages/node/6456955 |

**Disclaimer**

**The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.**