Advisory Alert

Alert Number: AAA20210213 **Date:** February 13, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
VMware	High	Command Injection Vulnerability

Description

Affected Product	VMware
Severity	High
Affected Vulnerabilities	Command Injection Vulnerability (CVE-2021-21976)
Description	VMware has released security patch updates addressing vulnerability that exist in their product. VMware vSphere Replication contains a post authentication command injection vulnerability in Startup Configuration page. A malicious actor with administrative access in vSphere Replication can execute shell commands on the underlying system. An attacker could exploit these vulnerabilities to perform remote code execution on an affected system. VMware highly recommends to apply relevant patches at earliest to avoid issues.
Affected Products	vSphere Replication
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2021-0001.html

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.