Advisory Alert

Alert Number: AAA20210524 **Date:** May 24, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**High**	Multiple Vulnerabilities
VMware	**Low**	Multiple out-of-bounds read vulnerabilities

Description

Affected Product	IBM
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-2161)
Description	IBM SDK, Java Technology Edition that is delivered with IBM WebSphere Application Server is affected by multiple vulnerabilities. This is due to an unspecified vulnerability in Java SE, Java SE Embedded, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries) which allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data. Thus these might affect some configurations of IBM WebSphere Application Server Traditional, IBM WebSphere Application Server Liberty and IBM WebSphere Application Server Hypervisor Edition.
Affected Products	WebSphere Application Server Liberty WebSphere Application Server version 9.0 WebSphere Application Server 8.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6454853

Affected Product	VMware
Severity	**Low**
Affected Vulnerability	Multiple out-of-bounds read vulnerabilities (CVE-2021-21987, CVE-2021-21988, CVE-2021-21989)
Description	VMware Workstation and Horizon Client for Windows affected by multiple out-of-bounds read vulnerabilities in the Cortado ThinPrint component. These issues exist in the TTC and JPEG2000 parsers. Upon a successful exploit of these vulnerabilities an attacker with access to a virtual machine or remote desktop may perform information disclosure from the TPView process running on the system where Workstation or Horizon Client for Windows is installed.
Affected Products	VMware Workstation Pro / Player (Workstation) VMware Horizon Client for Windows
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2021-0009.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.