# Advisory Alert

**Alert Number:** AAA20210310 **Date:** March 10, 2021

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

**Information Classification Level :** TLP: WHITE

## Overview

| Product | Severity | Vulnerability |
|---|---|---|
| **Microsoft** | **High** | Multiple Vulnerabilities |
| **Redhat** | **High** | Multiple Vulnerabilities |
| **IBM WebSphere** | **Medium** | Directory Traversal vulnerability |

## Description

| | |
|---|---|
| Affected Product | **Microsoft** |
| Severity | **High** |
| Affected Vulnerability | Multiple Vulnerabilities |
| Description | Microsoft has released its March 2021 Security Updates addressing multiple vulnerabilities that exists across windows operating systems and other softwares. A remote attacker can exploit some of these vulnerabilities to take control of an affected system. |
| Affected Products | Application Virtualization<br>Azure<br>Azure DevOps<br>Azure Sphere<br>Internet Explorer<br>Microsoft ActiveX<br>Microsoft Exchange Server<br>Microsoft Edge (Chromium-based)<br>Microsoft Graphics Component<br>Microsoft Office<br>Microsoft Office Excel<br>Microsoft Office PowerPoint<br>Microsoft Office SharePoint<br>Microsoft Office Visio<br>Microsoft Windows Codecs Library<br>Power BI<br>Role: DNS Server<br>Role: Hyper-V<br>Visual Studio<br>Windows Update Assistant<br>Windows Update Stack<br>Visual Studio Code<br>Windows Admin Center<br>Windows Container Execution Agent<br>Windows DirectX<br>Windows Error Reporting<br>Windows Event Tracing<br>Windows Extensible Firmware Interface<br>Windows Folder Redirection<br>Windows Installer<br>Windows Media<br>Windows Overlay Filter<br>Windows Print Spooler Components<br>Windows Projected File System Filter Driver<br>Windows Registry<br>Windows Remote Access API<br>Windows Storage Spaces Controller<br>Windows User Profile Service<br>Windows WalletService<br>Windows Win32K<br>Windows UPnP Device Host |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://msrc.microsoft.com/update-guide/releaseNote/2021-Mar |

| | |
|---|---|
| Affected Product | **Redhat** |
| Severity | **High** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2020-24394, CVE-2020-25212, CVE-2020-0444, CVE-2020-14351, CVE-2020-25211, CVE-2020-25705, CVE-29661) |
| Description | Redhat has released Security Updates addressing multiple vulnerabilities that exists with multiple Redhat products. Redhat highly recommends to apply necessary fixes at earliest to avoid issues. |
| Affected Products | Red Hat OpenShift Container Platform 4.4<br>Red Hat OpenShift Container Platform 4.5<br>Red Hat OpenShift Container Platform 4.6<br>Red Hat Enterprise MRG 2<br>Red Hat Enterprise Linux 5<br>Red Hat Enterprise Linux 6<br>Red Hat Enterprise Linux 7<br>Red Hat Enterprise Linux 7.4 Advanced Update Support<br>Red Hat Enterprise Linux 8<br>Red Hat Enterprise Linux 8.1 Extended Update Support<br>Red Hat Enterprise Linux 8.2 Extended Update Support |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://access.redhat.com/security/cve/CVE-2020-24394?extIdCarryOver=true&sc_cid=701f2000001OH6kAAG<br>https://access.redhat.com/security/cve/CVE-2020-25212?extIdCarryOver=true&sc_cid=701f2000001OH6kAAG<br>https://access.redhat.com/security/cve/CVE-2020-0444<br>https://access.redhat.com/security/cve/CVE-2020-14351<br>https://access.redhat.com/security/cve/CVE-2020-25211<br>https://access.redhat.com/security/cve/CVE-2020-25705<br>https://access.redhat.com/security/cve/CVE-2020-29661 |

| | |
|---|---|
| Affected Product | **IBM WebSphere** |
| Severity | **Medium** |
| Affected Vulnerability | Directory Traversal vulnerability (CVE-2020-5016) |
| Description | IBM WebSphere Application Server could allow a remote attacker to traverse directories on the system. When application security is disabled and JAX-RPC applications are present, an attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to view arbitrary xml files on the system. |
| Affected Products | WebSphere Application Server 9.0<br>WebSphere Application Server 8.5<br>WebSphere Application Server 8.0<br>WebSphere Application Server 7.0 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.ibm.com/support/pages/node/6427873 |

**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.**