Advisory Alert

Alert Number: AAA20230426 **Date:** April 26, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
VMware	**Critical**	Multiple Vulnerabilities
IBM	**High**	Multiple Vulnerabilities
Redhat	**High**, Medium	Multiple Vulnerabilities

Description

Affected Product	**VMware**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20869, CVE-2023-20870, CVE-2023-20871, CVE-2023-20872)
Description	VMware has released security updates for VMware Workstation and Fusion to address multiple vulnerabilities. **CVE-2023-20869 –** A Stack-based buffer-overflow vulnerability exists in the Bluetooth device-sharing functionality of VMware Workstation and VMware Fusion. This allows a malicious actor with local administrative privileges on a virtual machine to execute code as the virtual machine's VMX process running on the host. **CVE-2023-20870 -** An Information disclosure vulnerability exists in the Bluetooth device-sharing functionality of VMware Workstation and VMware Fusion. This allows a malicious actor with local administrative privileges on a virtual machine to read privileged information contained in hypervisor memory from a virtual machine. **CVE-2023-20871 -** A privilege escalation vulnerability exists in the VMware Fusion raw disk. A malicious actor with read/write access to the host operating system can elevate privileges to gain root access to the host operating system. **CVE-2023-20872 -** An Out-of-bounds read/write vulnerability exists in the in virtual SCSI CD/DVD device controller of VMware Workstation and VMware Fusion. A malicious attacker with access to a virtual machine that has a physical CD/DVD drive attached and configured to use a virtual SCSI controller may be able to execute code on the hypervisor from a virtual machine. VMware highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	VMware Workstation Pro and Player (versions 17.x) VMware Fusion (versions 13.x)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2023-0008.html#

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-27559, CVE-2023-29257, CVE-2023-29255, CVE-2023-26021 CVE-2023-25930, CVE-2023-26022, CVE-2023-27555)
Description	IBM has released security updates addressing multiple vulnerabilities in IBM DB2 and WebSphere products. These vulnerabilities could allow an attacker to cause denial of service and remote code execution attacks. IBM recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	IBM Db2 V10.5, V11.1, and V11.5 server editions on all platforms are affected. IBM WebSphere Remote Server 8.5, 9.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6986123 https://www.ibm.com/support/pages/node/6985667 https://www.ibm.com/support/pages/node/6985669 https://www.ibm.com/support/pages/node/6985681 https://www.ibm.com/support/pages/node/6985683 https://www.ibm.com/support/pages/node/6985687 https://www.ibm.com/support/pages/node/6985691

Affected Product	**Redhat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-0386, CVE-2022-43750, CVE-2023-28617)
Description	Red Hat has released several security advisories addressing multiple vulnerabilities in Red Hat Enterprise Linux (RHEL). **CVE-2023-0386 –** A flaw was found in the Linux kernel, where unauthorized access to the execution of the setuid file with capabilities was found in the Linux kernel's OverlayFS subsystem in how a user copies a capable file from a nosuid mount into another mount. This uid mapping bug allows a local user to escalate their privileges on the system. **CVE-2022-43750 -** An out-of-bounds memory write flaw exists in Linux kernel's USB Monitor component that allows a local user to crash or potentially escalate their privileges on the system. **CVE-2023-28617 -** A flaw was found in the Emacs text editor in the way it processes a specially crafted org-mode code with the function org-babel-execute:latex in ob-latex.el, which may lead to arbitrary command execution. Red Hat has released patches and updates to address these CVEs, and users are advised to apply these patches as soon as possible to ensure the security of their systems.
Affected Products	Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.0 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.0 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.0 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.0 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.0 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.0 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.0 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.0 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.0 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.0 aarch64 Red Hat Enterprise Linux Server for ARM 64 - 4 years of updates 9.0 aarch64 Red Hat Enterprise Linux Server for IBM z Systems - 4 years of updates 9.0 s390x Red Hat Enterprise Linux Server 7 x86_64 Red Hat Enterprise Linux Workstation 7 x86_64 Red Hat Enterprise Linux Desktop 7 x86_64 Red Hat Enterprise Linux for IBM z Systems 7 s390x Red Hat Enterprise Linux for Power, big endian 7 ppc64 Red Hat Enterprise Linux for Scientific Computing 7 x86_64 Red Hat Enterprise Linux for Power, little endian 7 ppc64le Red Hat Enterprise Linux for Real Time 7 x86_64 Red Hat Enterprise Linux for Real Time for NFV 7 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:1970 https://access.redhat.com/errata/RHSA-2023:1987 https://access.redhat.com/errata/RHSA-2023:1988 https://access.redhat.com/errata/RHSA-2023:2010

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.