Advisory Alert

Alert Number: AAA20230222 **Date:** February 22, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
VMware	**Critical**	Injection Vulnerability
VMware	**High**	XML External Entity Vulnerability
Redhat	**High , Medium**	Multiple Vulnerabilities
Zimbra	**Low**	Multiple Vulnerabilities

Description

Affected Product	**VMware**
Severity	**Critical**
Affected Vulnerability	Injection Vulnerability (CVE-2023-20858)
Description	VMware has released a security update addressing an injection vulnerability that exists in Carbon Black App Control. Using specially crafted input, a malicious user with privileged access to the APP Control Administration console may be able to gain access to the underling server operation system. VMware highly recommends to apply necessary fixes to avoid issues.
Affected Products	VMware Carbon Black App Control (App Control) Version 8.9.x , 8.8.x , 8.7.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2023-0004.html

Affected Product	**VMware**
Severity	**High**
Affected Vulnerability	XML External Entity Vulnerability (CVE-2023-20855)
Description	VMware has released a security update addressing the XML External Entity vulnerability in their products. Using specially crafted input, a malicious user with non-administrative access to vRealize Orchestrator can bypass XML parsing restrictions, leading to access to sensitive information or possible escalation of privileges. VMware recommends to apply necessary fixes to avoid issues.
Affected Products	VMware vRealize Orchestrator version 8.x running on Virtual Appliance VMware vRealize Automation 8.x VMware Cloud Foundation (Cloud Foundation) 4.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2023-0005.html

Affected Product	**Redhat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2006-20001, CVE-2022-2873, CVE-2022-2964, CVE-2022-3564, CVE-2022-36760, CVE-2022-37436, CVE-2022-41222, CVE-2022-4139, CVE-2022-4378, CVE-2022-43945, CVE-2022-4415, CVE-2022-47629, CVE-2023-22809)
Description	Redhat has released security updates addressing multiple vulnerabilities in their products. If exploited these vulnerabilities could lead to out-of-bounds memory access, integer overflow, privilege escalation and denial of service. Redhat recommends to apply necessary fixes to avoid issues.
Affected Products	Red Hat CodeReady Linux Builder for ARM 64 8 aarch64 Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le Red Hat CodeReady Linux Builder for x86_64 8 x86_64 Red Hat Enterprise Linux for ARM 64 8 aarch64 Red Hat Enterprise Linux for IBM z Systems 8 s390x Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for Real Time 8 x86_64 Red Hat Enterprise Linux for Real Time for NFV 8 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.1 x86_64 Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.1 ppc64le Red Hat Virtualization 4 for RHEL 8 x86_64 Red Hat Virtualization Host 4 for RHEL 8 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:0859 https://access.redhat.com/errata/RHSA-2023:0858 https://access.redhat.com/errata/RHSA-2023:0856 https://access.redhat.com/errata/RHSA-2023:0854 https://access.redhat.com/errata/RHSA-2023:0852 https://access.redhat.com/errata/RHSA-2023:0839 https://access.redhat.com/errata/RHSA-2023:0837 https://access.redhat.com/errata/RHSA-2023:0832

Affected Product	**Zimbra**
Severity	**Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-0286, CVE-2022-4304, CVE-2018-25032)
Description	Zimbra has released security updates addressing multiple vulnerabilities that exist in their products. If exploited these vulnerabilities could lead to out-of-bounds access, denial of services, read memory contents and Information Exposure. **CVE-2023-0286-** A vulnerability was found in X.400 address processing inside an X.509 GeneralName. If exploited an attacker can pass arbitrary pointers to a memcmp call, enabling them to read memory contents or enact a denial of service. **CVE-2022-4304-** A vulnerability was found in timing based side channel exists in the OpenSSL RSA Decryption implementation. A remote attacker can perform a Bleichenbacher style attack and decrypt data sent over the network by sending large number of trial messages. **CVE-2018-25032-** The vulnerability exists due to insufficient validation of user-supplied input when compressing data. A remote attacker can pass specially crafted input to the application, trigger memory corruption and perform a denial of service (DoS) attack. Zimbra recommends to apply necessary fixes to avoid issues.
Affected Products	Zimbra Collaboration Joule 8.8.15 Zimbra Collaboration Kepler 9.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P37#Security_Fixes https://wiki.zimbra.com/wiki/Zimbra_Releases/9.0.0/P30#Security_Fixes

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.