Advisory Alert

Alert Number: AAA20230125 **Date:** January 25, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
VMware	**Critical**	Multiple Vulnerabilities
Dell	**High**, Medium	Multiple Vulnerabilities
Redhat	**High**, Medium	Multiple Vulnerabilities
IBM	Medium	Server-Side Request Forgery Vulnerability

Description

Affected Product	**VMware**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-31706, CVE-2022-31704, CVE-2022-31710, CVE-2022-31711)
Description	VMware has released a security update addressing multiple vulnerabilities that exist in VMware vRealize Log Insight. **CVE-2022-31706**- A Directory Traversal Vulnerability allows an unauthenticated, malicious actor to inject files into the operating system of an impacted appliance which may lead to remote code execution. **CVE-2022-31704**- A Broken access control Vulnerability allows an unauthenticated, malicious actor to inject files into the operating system of an impacted appliance which may lead to remote code execution. **CVE-2022-31710**- A Deserialization Vulnerability allows an unauthenticated, malicious actor to remotely trigger the deserialization of untrusted data which could lead to a denial of service **CVE-2022-31711**- A Information Disclosure Vulnerability allows an unauthenticated, malicious actor to collect sensitive session and application information VMware highly recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	VMware vRealize Log Insight
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2023-0001.html

Affected Product	**Dell**
Severity	**High**, Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-26316, CVE-2021-26346, CVE-2017-5717, CVE-2022-30773, CVE-2022-30774, CVE-2022-31243, CVE-2022-32266, CVE-2022-32267, CVE-2022-33905, CVE-2022-33906, CVE-2022-33907, CVE-2022-33908, CVE-2022-33909, CVE-2022-33982, CVE-2022-33983, CVE-2022-33984, CVE-2022-33985, CVE-2022-33986, CVE-2022-34325, CVE-2022-33973, CVE-2022-34463)
Description	Dell has released security updates addressing multiple vulnerabilities in their products. Most severe vulnerabilities could lead to arbitrary code execution, privilege escalation, SMRAM corruption and information disclosure. Dell recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	Inspiron 3481, 3505, 3515, 3525, 3581, 3585, 3781, 3785, 5405, 5415, 5425, 5485, 5485 2-in-1, 5505, 5515, 5570, 5585, 5770, 7405 2-in-1, 7415, 7425 Latitude 12 Rugged Tablet 7212, 13 3380, 3180, 3189, 3190, 3190 2-in-1, 3300, 3390 2-in-1, 3490, 3590, 5280, 5285 2-in-1, 5288, 5289, 5290, 5290 2-in-1, 5400, 5414 Rugged, 5420 Rugged, 5424 Rugged, 5480, 5488, 5490, 5580, 5590, 7200 2-in-1, 7210 2-in-1, 7212 Rugged Extreme Tablet, 7214 Rugged Extreme, 7275 2-in-1, 7280, 7285, 7285 2-in-1, 7290, 7320 Detachable, 7370, 7380, 7389, 7390, 7390 2-in-1, 7414 Rugged Extreme, 7424 Rugged Extreme, 7480, 7490, Rugged 7220, Rugged 7220EX, 3480, 3580 OptiPlex 3050, 3050 All-In-One, 5050, 5250, 7050, 7450, Vostro 3267, 3268, 3405, 3425, 3481, 3515, 3525, 3581, 3584, 3667, 3668, 3669, 5415, 5515, 5625, Wyse 7040 Thin Client XPS 13 9315 2-in-1 XPS 15 9575 2-in-1 Dell G15 5515, G15 5525, G5 5505 Edge Gateway 3000 and 5000 series Embedded Box PC 3000, PC 5000
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000207757/dsa-2023-023-dell-client-bios-security-update-for-amd-client-vulnerabilities https://www.dell.com/support/kbdoc/en-us/000207439/dsa-2023-013 https://www.dell.com/support/kbdoc/en-us/000207529/dsa-2023-012 https://www.dell.com/support/kbdoc/en-us/000207386/dsa-2023-009 https://www.dell.com/support/kbdoc/en-us/000207385/dsa-2023-008-dell-client-security-update-for-dell-client-bios https://www.dell.com/support/kbdoc/en-us/000207385/dsa-2023-008-dell-client-security-update-for-dell-client-bios

Affected Product	**Redhat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-4139, CVE-2022-26373, CVE-2022-4254, CVE-2022-4144, CVE-2022-2964, CVE-2021-25220, CVE-2022-2795, CVE-2021-26401)
Description	Redhat has released a security update addressing multiple vulnerabilities that exists in their products. If exploited these vulnerabilities could cause system crash, privilege escalation, domain takeover and out-of-bounds reads and writes Redhat highly recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 8.6 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 8.6 s390x Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 8.6 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 8.6 x86_64 Red Hat Enterprise Linux Desktop 7 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.6 aarch64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.6 s390x 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 Power, little endian - Extended Update Support 8.6 ppc64le Red Hat Enterprise Linux for Power, little endian 7 ppc64le Red Hat Enterprise Linux for Real Time - Telecommunications Update Service 8.2 x86_64 Red Hat Enterprise Linux for Real Time 7 x86_64 Red Hat Enterprise Linux for Real Time for NFV - Telecommunications Update Service 8.2 x86_64 Red Hat Enterprise Linux for Real Time for NFV 7 x86_64 Red Hat Enterprise Linux for Scientific Computing 7 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.6 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 - Update Services for SAP Solutions 8.2 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6 x86_64 Red Hat Enterprise Linux Server - AUS 8.2 x86_64, AUS 8.6 x86_64, TUS 8.2 x86_64, TUS 8.6 x86_64 Red Hat Enterprise Linux Server 7 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.1 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.2 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le Red Hat Enterprise Linux Workstation 7 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-2023:0441 https://access.redhat.com/errata/RHSA-2023:0440 https://access.redhat.com/errata/RHSA-2023:0442 https://access.redhat.com/errata/RHSA-2023:0432 https://access.redhat.com/errata/RHSA-2023:0432 https://access.redhat.com/errata/RHSA-2023:0404 https://access.redhat.com/errata/RHSA-2023:0403 https://access.redhat.com/errata/RHSA-2023:0402 https://access.redhat.com/errata/RHSA-2023:0400 https://access.redhat.com/errata/RHSA-2023:0399 https://access.redhat.com/errata/RHSA-2023:0396 https://access.redhat.com/errata/RHSA-2023:0397 https://access.redhat.com/errata/RHSA-2023:0395 https://access.redhat.com/errata/RHSA-2023:0392

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Server-Side Request Forgery (CVE-2022-35282)
Description	IBM has released a security update addressing a Server-Side Request Forgery vulnerability that exists in IBM WebSphere Application Server which is a component of IBM Operations Analytics Predictive Insights. **CVE-2022-35282 -** An attacker with local network access can craft request to obtain sensitive data. IBM recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	IBM Operations Analytics Predictive Insights – All with Websphere Application Server 9.0 IBM Operations Analytics Predictive Insights – All with Websphere Application Server 8.5 IBM Operations Analytics Predictive Insights – All with Websphere Application Server 8.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6857243

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.