Advisory Alert

Alert Number: AAA20241219 **Date:** December 19, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Apache Struts	**Critical**	Path Traversal Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
FortiGuard	**Critical**	Unauthenticated Limited File Read Vulnerability
IBM	**Critical**	Remote Arbitrary Command Execution Vulnerability
SUSE	**High**	Multiple Vulnerabilities
FortiGuard	**High**, Medium	Multiple Vulnerabilities
Apache Tomcat	**High**, Low	Multiple Vulnerabilities
Red Hat	Medium	Memory Corruption Vulnerability

Description

Affected Product	**Apache Struts**
Severity	**Critical**
Affected Vulnerability	Path Traversal Vulnerability (CVE-2024-53677)
Description	Apache has released security updates addressing a Path Traversal Vulnerability that exists in Apache Struts. **CVE-2024-53677** - An attacker can manipulate file upload params to enable paths traversal and under some circumstances this can lead to uploading a malicious file which can be used to perform Remote Code Execution. Apache advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Struts 2.0.0 through Struts 2.3.37 (EOL) Struts 2.5.0 through Struts 2.5.33 (EOL) Struts 6.0.0 through Struts 6.3.0.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://cwiki.apache.org/confluence/display/WW/S2-067

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-23450, CVE-2021-33036, CVE-2021-25642, CVE-2024-35328, CVE-2024-35325, CVE-2024-35326, CVE-2024-32888, CVE-2024-2004, CVE-2024-2398, CVE-2024-21769, CVE-2024-21807, CVE-2024-22374, CVE-2024-22376, CVE-2024-23497, CVE-2024-24986, CVE-2024-21801, CVE-2024-21806, CVE-2024-21810, CVE-2024-23499, CVE-2024-23981, CVE-2024-24983, CVE-2023-49141, CVE-2024-6387, CVE-2024-21829, CVE-2024-21781, CVE-2024-23984, CVE-2024-24968, CVE-2024-21853, CVE-2024-47483, CVE-2024-47481)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in third party products which affect Dell Data Lakehouse System Software. These vulnerabilities could be exploited by malicious users to compromise the affected system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	DELL Data Lakehouse System Software Versions 1.0.0.0 and 1.1.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000240535/dsa-2024-419-security-update-for-dell-data-lakehouse-system-software-for-multiple-third-party-component-vulnerabilities

Affected Product	**FortiGuard**
Severity	**Critical**
Affected Vulnerability	Unauthenticated Limited File Read Vulnerability (CVE-2023-34990)
Description	FortiGuard has released security updates addressing an Unauthenticated Limited File Read Vulnerability that exists in FortiWLM. Exploitation of this vulnerability leads to a relative path traversal which may allow a remote unauthenticated attacker to read sensitive files. FortiGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	FortiWLM 8.6 - versions 8.6.0 through 8.6.5 FortiWLM 8.5 - versions 8.5.0 through 8.5.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-23-144

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Remote Arbitrary Command Execution (CVE-2015-7450)
Description	IBM has released security updates addressing a Remote Arbitrary Command Execution Vulnerability that exists in WebSphere Application Server shipped with WebSphere Remote Server. **CVE-2015-7450** - Serialized-object interfaces in certain IBM analytics, business solutions, cognitive, IT infrastructure, and mobile and social products allow remote attackers to execute arbitrary commands via a crafted serialized Java object, related to the InvokerTransformer class in the Apache Commons Collections library. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM WebSphere Remote Server - Product Family version 9.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/1111257

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause memory leak, system crash, use-after-free conditions. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.5 Public Cloud Module 15-SP5 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise Server 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2024/suse-su-20244376-1/

Affected Product	**FortiGuard**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-48889, CVE-2024-50570)
Description	FortiGuard has released security updates addressing multiple vulnerabilities that exist in FortiManager and FortiClient. **CVE-2024-48889** - An Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in FortiManager may allow an authenticated remote attacker to execute unauthorized code via FGFM crafted requests. **CVE-2024-50570** - A Cleartext Storage of Sensitive Information vulnerability in FortiClient Windows may permit a local authenticated user to retrieve VPN password via memory dump, due to JavaScript's garbage collector. FortiGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	FortiManager 7.6 - version 7.6.0 FortiManager 7.4 - versions 7.4.0 through 7.4.4 FortiManager 7.4 Cloud - versions 7.4.1 through 7.4.4 FortiManager 7.2 - versions 7.2.3 through 7.2.7 FortiManager 7.2 Cloud - versions 7.2.1 through 7.2.7 FortiManager 7.0 - versions 7.0.5 through 7.0.12 FortiManager 7.0 Cloud - versions 7.0.1 through 7.0.12 FortiManager 6.4 - versions 6.4.10 through 6.4.14 FortiClientLinux 7.4 - versions 7.4.0 through 7.4.2 FortiClientLinux 7.2 - versions 7.2.0 through 7.2.7 FortiClientLinux 7.0 - versions 7.0.0 through 7.0.13 FortiClientWindows 7.4 - versions 7.4.0 through 7.4.1 FortiClientWindows 7.2 - versions 7.2.0 through 7.2.6 FortiClientWindows 7.0 - versions 7.0.0 through 7.0.13
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.fortiguard.com/psirt/FG-IR-24-425 • https://www.fortiguard.com/psirt/FG-IR-23-278

Affected Product	**Apache Tomcat**
Severity	**High**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-54677, CVE-2024-50379)
Description	Apache has released security updates addressing multiple vulnerabilities that exist in Apache Tomcat. **CVE-2024-54677** - Uncontrolled Resource Consumption vulnerability in the examples web application provided with Apache Tomcat leads to denial of service. **CVE-2024-50379** - Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability during JSP compilation in Apache Tomcat permits an RCE on case insensitive file systems when the default servlet is enabled for write (non-default configuration). Apache advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Apache Tomcat 11 versions 11.0.0-M1 to 11.0.1 Apache Tomcat 10 versions 10.1.0-M1 to 10.1.33 Apache Tomcat 9 versions 9.0.0.M1 to 9.0.97
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.2 • https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.34 • https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.98

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Memory Corruption Vulnerability (CVE-2024-40989)
Description	Red Hat has released security updates to address a vulnerability in multiple Red Hat products that could potentially lead to memory corruption. **CVE-2024-40989** - A vulnerability was found in the Linux kernel's KVM for ARM64 within the vgic-init.c, vgic-mmio-v3.c, and vgic.h files. The virtual vCPUs may retain dangling pointers in a redistributor region after they have been torn down, leading to potential memory corruption. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.2 x86_64 Red Hat Enterprise Linux Server - AUS 9.2 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.2 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.2 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.2 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.2 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.2 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.2 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.2 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2024:11482

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.