Advisory Alert

Alert Number: AAA20240821 **Date:** August 21, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
ManageEngine	**High**	Multiple SQL Injection Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
HPE	**High**	Local Escalation of Privilege Vulnerability
SUSE	**High**	Multiple Vulnerabilities
Dell	**High**, Medium	Multiple Vulnerabilities
Oracle	**High**, Medium	Multiple Vulnerabilities
IBM	Medium	Multiple Denial Of Service Vulnerabilities
Joomla	Medium, Low	Multiple Vulnerabilities

Description

Affected Product	**ManageEngine**
Severity	**High**
Affected Vulnerability	Multiple SQL Injection Vulnerabilities (CVE-2024-5586, CVE-2024-5467)
Description	ManageEngine has released security updates addressing multiple SQL Injection Vulnerabilities that exist in ADAudit Plus. These vulnerabilities could allow an authenticated adversary to execute custom queries and access the database table entries using the vulnerable request. ManageEngine advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	All ADAudit Plus builds below 8121
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.manageengine.com/products/active-directory-audit/cve-2024-5586.html • https://www.manageengine.com/products/active-directory-audit/cve-2024-5467.html

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-52463, CVE-2023-52735, CVE-2024-26853, CVE-2024-36000, CVE-2024-36883, CVE-2024-38608, CVE-2024-40995, CVE-2024-41076, CVE-2024-41090, CVE-2024-41091, CVE-2024-42107)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Denial of Service, memory leak, out-of-bounds access conditions. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.2 x86_64 Red Hat Enterprise Linux for Real Time for NFV for x86_64 - 4 years of updates 9.2 x86_64 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-2024:5673 • https://access.redhat.com/errata/RHSA-2024:5672

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Local Escalation of Privilege Vulnerability (CVE-2024-24853)
Description	HPE has released security updates addressing a Local Escalation of Privilege Vulnerability that exists in their products. **CVE-2024-24853** - Incorrect behavior order in transition between executive monitor and SMI transfer monitor (STM) in some Intel(R) Processor may allow a privileged user to potentially enable escalation of privilege via local access. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE ProLiant DL20 Gen10 Plus server - Prior to v2.20_08-07-2024 HPE ProLiant DL110 Gen10 Plus Telco server - Prior to v2.20_08-07-2024 HPE ProLiant DL360 Gen10 Plus server - Prior to v2.20_08-07-2024 HPE ProLiant DL380 Gen10 Plus server - Prior to v2.20_08-07-2024 HPE ProLiant ML30 Gen10 Plus server - Prior to v3.40_08-01-2024 HPE ProLiant MicroServer Gen10 Plus v2 - Prior to v2.20_08-07-2024 HPE Apollo 4200 Gen10 Plus System - Prior to v2.20_08-07-2024 HPE ProLiant XL220n Gen10 Plus Server - Prior to v2.20_08-07-2024 HPE ProLiant XL290n Gen10 Plus Server - Prior to v2.20_08-07-2024 HPE Synergy 480 Gen10 Plus Compute Module - Prior to v2.20_08-07-2024 HPE Edgeline e920 Server Blade - Prior to v2.20_08-07-2024 HPE Edgeline e920d Server Blade - Prior to v2.20_08-07-2024 HPE Edgeline e920t Server Blade - Prior to v2.20_08-07-2024 HPE ProLiant m750 Server Blade - Prior to v3.40_08-01-2024 HPE ProLiant MicroServer Gen10 Plus - Prior to v3.40_08-01-2024 HPE ProLiant ML30 Gen10 Server - Prior to v3.40_08-01-2024 HPE ProLiant DL20 Gen10 Server - Prior to v3.40_08-01-2024
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04681en_us&docLocale=en_US

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 configuration modification, system crash, information disclosure. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.4, 15.6 SUSE Linux Enterprise Desktop 15 SP4 LTSS 15-SP4 SUSE Linux Enterprise High Performance Computing 15 SP4 SUSE Linux Enterprise High Performance Computing ESPOS 15 SP4 SUSE Linux Enterprise High Performance Computing LTSS 15 SP4 SUSE Linux Enterprise Live Patching 15-SP6 SUSE Linux Enterprise Micro 5.3, 5.4 SUSE Linux Enterprise Micro for Rancher 5.3, 5.4 SUSE Linux Enterprise Real Time 15 SP6 SUSE Linux Enterprise Server 15 SP4, 15 SP6 SUSE Linux Enterprise Server 15 SP4 LTSS 15-SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP4, 15 SP6 SUSE Manager Proxy 4.3 SUSE Manager Retail Branch Server 4.3 SUSE Manager Server 4.3 SUSE Real Time Module 15-SP6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20242973-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20242980-1/

Affected Product	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-45733, CVE-2023-46103, CVE-2023-39230, CVE-2022-43456)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. 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	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000222726/dsa-2024-113-security-update-for-dell-client-platform-for-intel-processor-and-intel-core-ultra-processor-advisories • https://www.dell.com/support/kbdoc/en-us/000226009/dsa-2024-271-security-update-for-dell-client-platform-for-multiple-intel-rapid-storage-technology-software-vulnerabilities

Affected Product	**Oracle**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-25111, CVE-2024-32487, CVE-2023-40030)
Description	Oracle has released security updates addressing multiple vulnerabilities that exist in Oracle Solaris. These vulnerabilities could be exploited by malicious users to compromise the affected system. Oracle advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Oracle Solaris 11.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.oracle.com/security-alerts/bulletinjul2024.html

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Multiple Denial Of Service Vulnerabilities (CVE-2024-37529, CVE-2024-35136)
Description	IBM has released security updates addressing multiple Denial Of Service Vulnerabilities that exist in IBM Db2. **CVE-2024-37529** - IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) could allow an authenticated user to cause a denial of service with a specially crafted query due to improper memory allocation. **CVE-2024-35136** - IBM Db2 for Linux, UNIX and Windows (includes DB2 Connect Server) federated server is vulnerable to denial of service with a specially crafted query under certain conditions. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Db2 versions 10.5.0 - 10.5.11, 11.1.4 - 11.1.4.7 and 11.5.0 - 11.5.9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7165343 • https://www.ibm.com/support/pages/node/7165341

Affected Product	**Joomla**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-40743, CVE-2024-27187, CVE-2024-27186, CVE-2024-27185, CVE-2024-27184)
Description	Joomla has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Cross-site Scripting, Cache Poisoning and URL redirects. Joomla advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Joomla CMS versions 3.0.0-3.10.16-elts, 4.0.0-4.4.6 and 5.0.0-5.1.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://developer.joomla.org/security-centre/946-20240805-core-xss-vectors-in-outputfilter-strip-methods.html • https://developer.joomla.org/security-centre/945-20240804-core-improper-acl-for-backend-profile-view.html • https://developer.joomla.org/security-centre/944-20240803-core-xss-in-html-mail-templates.html • https://developer.joomla.org/security-centre/942-20240802-core-cache-poisoning-in-pagination.html • https://developer.joomla.org/security-centre/941-20240801-core-inadequate-validation-of-internal-urls.html

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.