Advisory Alert

Alert Number: **AAA20240508** **Date:** **May 8, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	SQL Injection Vulnerability
Veeam	**High**	Remote Code Execution Vulnerability
SUSE	**High**	Multiple Vulnerabilities
Red Hat	**High, Medium**	Multiple Vulnerabilities
Dell	**Medium, Low**	Multiple Vulnerabilities
Ubuntu	**Medium, Low**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has issued a Critical security update addressing multiple vulnerabilities that exist in third party components used in Multiple Dell 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	• Dell Avamar Server Hardware Appliance Gen4T/Gen5A Version 19.4, 19.7, 19.8, 19.9, 19.10 running SUSE Linux Enterprise 12 SP5 • Dell Avamar Virtual Edition Version 19.4, 19.7, 19.8, 19.9, 19.10 running SUSE Linux Enterprise 12 SP5 (including Azure and AWS deployments) • Dell Avamar NDMP Accelerator Version 19.4, 19.7, 19.8, 19.9, 19.10 running SUSE Linux Enterprise 12 SP5 • Dell Avamar VMware Image Proxy Version 19.4, 19.7, 19.8, 19.9, 19.10 running SUSE Linux Enterprise 12 SP5 • Dell Networker Virtual Edition (NVE) Versions 19.4.x, 19.5.x, 19.6.x, 19.7.x, 19.8.x, 19.9.x, 19.10.x running SUSE Linux Enterprise 12 SP5 • Dell Power Protect DP Series Appliance / Dell Integrated Data Protection Appliance (IDPA) Version 2.7.x running on SLES12SP5 • Dell PowerProtect Data Manager DM5500 Appliance Versions 5.15 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000224827/dsa-2024-198-security-update-for-dell-avamar-dell-networker-virtual-edition-nve-and-dell-powerprotect-dp-series-appliance-dell-integrated-data-protection-appliance-idpa-security-update-for-multiple-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000224843/dsa-2024-083-security-update-for-dell-powerprotect-data-manager-appliance-for-multiple-vulnerabilities

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	SQL Injection Vulnerability (CVE-2024-1597)
Description	IBM has released a security update addressing an SQL Injection Vulnerability that exists in PostgreSQL affects IBM Storage Scale. A remote attacker could send specially crafted SQL statements when using the non-default connection property preferQueryMode=simple in combination with application code that has a vulnerable SQL that negates a parameter value, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Scale 5.1.0.0 - 5.1.9.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7150357

Affected Product	**Veeam**
Severity	**High**
Affected Vulnerability	Remote Code Execution Vulnerability (CVE-2024-29212)
Description	Veeam has released a security update addressing Remote Code Execution Vulnerability that exists in Veeam Service Provider Console. Due to an unsafe deserialization method used by the Veeam Service Provider Console (VSPC) server in communication between the management agent and its components, under certain conditions, it is possible to perform Remote Code Execution (RCE) on the VSPC server machine. Veeam advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Veeam Service Provider Console 4.0 , 5.0 , 6.0 , 7.0 , 8.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.veeam.com/kb4575

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-5717,CVE-2024-0775,CVE-2024-1086)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Heap out-of-bounds write and Use-After-Free conditions. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SUSE Linux Enterprise High Performance Computing 15 SP2 SUSE Linux Enterprise Live Patching 15-SP2 SUSE Linux Enterprise Server 15 SP2 SUSE Linux Enterprise Server for SAP Applications 15 SP2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20241551-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20241545-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20241537-1/

Affected Product	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-6240, CVE-2024-2004, CVE-2024-23672, CVE-2024-2379, CVE-2024-2398, CVE-2024-2466, CVE-2024-25742, CVE-2024-25743, CVE-2024-27316, CVE-2024-28182)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. If Exploited, these vulnerabilities could lead to Denial of Service, Arbitrary Code Execution Improper Certificate Validation Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	JBoss Enterprise Web Server 5 for RHEL 7 x86_64 JBoss Enterprise Web Server 5 for RHEL 8 x86_64 JBoss Enterprise Web Server 5 for RHEL 9 x86_64 JBoss Enterprise Web Server 6 for RHEL 8 x86_64 JBoss Enterprise Web Server 6 for RHEL 9 x86_64 JBoss Enterprise Web Server Text-Only Advisories x86_64 Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat CodeReady Linux Builder for ARM 64 9 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.4 s390x Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.4 x86_64 Red Hat CodeReady Linux Builder for x86_64 9 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat Enterprise Linux for ARM 64 9 aarch64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x Red Hat Enterprise Linux for IBM z Systems 9 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Enterprise Linux for Real Time 9 x86_64 Red Hat Enterprise Linux for Real Time for NFV 9 x86_64 Red Hat Enterprise Linux for Real Time for NFV for x86_64 - 4 years of updates 9.4 x86_64 Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.4 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64 Red Hat Enterprise Linux for x86_64 9 x86_64 Red Hat Enterprise Linux Server - AUS 9.4 x86_64 Red Hat Enterprise Linux Server for ARM 64 - 4 years of updates 9.4 aarch64 Red Hat Enterprise Linux Server for IBM z Systems - 4 years of updates 9.4 s390x Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le Red Hat JBoss Core Services 1 for RHEL 7 x86_64 Red Hat JBoss Core Services 1 for RHEL 8 x86_64 Red Hat JBoss Core Services Text-Only Advisories x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2024:2758 • https://access.redhat.com/errata/RHSA-2024:2694 • https://access.redhat.com/errata/RHSA-2024:2693 • https://access.redhat.com/errata/RHSA-2024:1917 • https://access.redhat.com/errata/RHSA-2024:1916 • https://access.redhat.com/errata/RHSA-2024:1914 • https://access.redhat.com/errata/RHSA-2024:1913

Affected Product	**Dell**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-28971, CVE-2024-25967, CVE-2024-25970, CVE-2024-25969, CVE-2024-25965, CVE-2024-25968, CVE-2024-25966)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause privilege escalation, denial of service and information disclosure. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PowerScale OneFS Version 8.2.x through 9.3.0.0 PowerScale OneFS Version 9.4.0.0 through 9.4.0.17 PowerScale OneFS Version 9.5.0.0 through 9.5.0.7 PowerScale OneFS Version 9.6.0.x through 9.7.0.1 PowerScale OneFS Version 9.7.0.2 Dell Update Manager Plugin Versions 1.4.0 through 1.5.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000224860/dsa-2024-163-security-update-for-dell-powerscale-onefs-for-multiple-security-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000224849/dsa-2024-209-security-update-for-dell-update-manager-plugin-vulnerability

Affected Product	**Ubuntu**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in Ubuntu Linux kernel. These vulnerabilities could be exploited by malicious users to cause Denial of Service, Sensitive Information Disclosure, Arbitrary Code Execution, authentication bypass. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 22.04 Ubuntu 20.04 Ubuntu 18.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-6765-1 • https://ubuntu.com/security/notices/USN-6766-1 • https://ubuntu.com/security/notices/USN-6767-1

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.