Advisory Alert

Alert Number: AAA20240716 **Date:** July 16, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Prototype Pollution Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
Suse	**High**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities
HPE	**Medium**	Multiple Denial of Service Vulnerabilities
IBM	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-41993, CVE-2024-21892, CVE-2024-20954, CVE-2024-21098, CVE-2024-21085, CVE-2024-21011, CVE-2024-21068, CVE-2024-21094, CVE-2024-21003, CVE-2024-21005, CVE-2024-21002, CVE-2024-21004, CVE-2022-3491, CVE-2022-3520, CVE-2022-3591, CVE-2022-3705, CVE-2022-4141, CVE-2022-4292, CVE-2022-4293, CVE-2023-0049, CVE-2023-0051, CVE-2023-0054, CVE-2023-0288, CVE-2023-0433, CVE-2024-22667, CVE-2022-1968, CVE-2022-0213, CVE-2021-4136, CVE-2022-2286, CVE-2022-2124, CVE-2022-0261, CVE-2022-2304, CVE-2022-2206, CVE-2022-1616, CVE-2022-0318, CVE-2021-4019, CVE-2021-3984, CVE-2022-0413, CVE-2021-3778, CVE-2021-3872, CVE-2022-2345, CVE-2022-2125, CVE-2022-0392, CVE-2022-2284, CVE-2022-2257, CVE-2022-1720, CVE-2022-0128, CVE-2022-2175, CVE-2022-2343, CVE-2022-2210, CVE-2022-2182, CVE-2022-2126, CVE-2022-1927, CVE-2022-2285, CVE-2021-3974, CVE-2022-0407, CVE-2022-2129, CVE-2021-3796, CVE-2022-1735, CVE-2021-3968, CVE-2022-1897, CVE-2022-1796, CVE-2022-0361, CVE-2022-1619, CVE-2021-4069, CVE-2022-1851, CVE-2022-0359, CVE-2021-3973, CVE-2021-3927, CVE-2022-2264, CVE-2022-1898, CVE-2022-2183, CVE-2022-1381, CVE-2022-2344, CVE-2022-2207, CVE-2021-4192, CVE-2022-2068, CVE-2022-1292, CVE-2024-26717, CVE-2023-7192, CVE-2022-1679, CVE-2022-20292, CVE-2022-0847, CVE-2022-0492, CVE-2022-1652, CVE-2021-4197, CVE-2022-1048, CVE-2021-4083, CVE-2023-48795, CVE-2023-46445, CVE-2023-46446, CVE-2021-30560, CVE-2022-27239, CVE-2022-23219, CVE-2022-23218, CVE-2021-45078, CVE-2022-2440, CVE-2021-43527, CVE-2022-24903, CVE-2022-1304, CVE-2017-7555, CVE-2022-24407, CVE-2022-3696, CVE-2023-0286, CVE-2022-27774, CVE-2023-38545, CVE-2023-38546, CVE-2023-28319, CVE-2023-28320, CVE-2023-28321, CVE-2023-28322, CVE-2020-25717, CVE-2020-35524, CVE-2020-35523, CVE-2022-29155, CVE-2020-0452, CVE-2023-45853, CVE-2021-44832, CVE-2023-22025, CVE-2023-22067, CVE-2023-22081, CVE-2023-46218, CVE-2023-46219)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in third party components which affect 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 Data Protection Search - Versions 19.3.0, 19.4.0, 19.5.0, 19.5.1, 19.6.0, 19.6.1, 19.6.2 - 19.6.4 IDPA - Versions prior to 2.7.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000226918/dsa-2024-031-security-update-for-dell-data-protection-search-for-multiple-third-party-component-vulnerabilities

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Prototype Pollution Vulnerability (CVE-2023-36665)
Description	IBM has released security update addressing a Prototype Pollution Vulnerability that exists in Grafana which affect IBM Storage Ceph products. This vulnerability could allow a remote attacker to execute arbitrary code on the system by sending a specially crafted message. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Ceph - Version(s) 7.0z1 - z2, 6.1z1 - z5, 6.0, 5.3z1 - z6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7160167

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-47548, CVE-2021-47596, CVE-2022-48627, CVE-2023-52638, CVE-2024-26583, CVE-2024-26585, CVE-2024-26720, CVE-2024-26783, CVE-2024-26801, CVE-2024-26852, CVE-2024-35857, CVE-2024-35898, CVE-2024-35969, CVE-2024-36005, CVE-2024-36016, CVE-2024-36886)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exists in the Red Hat Products. These vulnerabilities could be exploited by malicious users to cause Use After Free Conditions, Remote Code Execution, NULL Dereferences, Race Conditions. 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 Server for ARM 64 - 4 years of updates 9.2 aarch64 Red Hat Enterprise Linux Server 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-2024:4533

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-26828, CVE-2024-26923, CVE-2024-23307, CVE-2024-26828, CVE-2024-26923, CVE-2024-23307, CVE-2024-26828, CVE-2024-26923, CVE-2024-26930)
Description	SUSE has released security updates addressing multiple vulnerabilities that exists in their products. Exploitation of these vulnerabilities may compromise the affected system. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	OpenSUSE Leap 15.5 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise Live Patching 15-SP5 SUSE Linux Enterprise Micro 5.5 SUSE Linux Enterprise Real Time 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-20242480-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242487-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242488-1

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-24861, CVE-2024-25739, CVE-2024-26810, CVE-2024-35910, CVE-2024-35935, CVE-2024-35970, CVE-2024-35976, CVE-2024-35990, CVE-2023-52488, CVE-2024-26950, CVE-2024-26922, CVE-2024-26994, CVE-2024-27018, CVE-2024-35813, CVE-2024-35853, CVE-2024-35893, CVE-2024-27016, CVE-2024-36006, CVE-2024-35922, CVE-2024-35804, CVE-2024-26958, CVE-2024-26642, CVE-2024-26828, CVE-2024-26977, CVE-2024-35796, CVE-2024-35933, CVE-2024-35789, CVE-2024-27020, CVE-2024-35852, CVE-2024-35885, CVE-2024-27000, CVE-2024-35815, CVE-2024-27009, CVE-2024-36004, CVE-2024-35918, CVE-2024-26812, CVE-2024-35944, CVE-2024-26935, CVE-2024-26629, CVE-2024-36020, CVE-2024-27013, CVE-2024-35955, CVE-2024-35930, CVE-2024-26925, CVE-2024-26964, CVE-2024-24857, CVE-2024-35823, CVE-2024-35900, CVE-2024-36008, CVE-2024-35989, CVE-2024-26996, CVE-2023-52699, CVE-2024-26974, CVE-2024-26955, CVE-2024-35822, CVE-2024-26926, CVE-2024-35857, CVE-2024-35940, CVE-2024-26976, CVE-2024-35890, CVE-2024-27015, CVE-2024-35879, CVE-2024-26937, CVE-2024-35791, CVE-2024-35899, CVE-2024-35907, CVE-2024-35938, CVE-2024-36031, CVE-2024-35785, CVE-2024-27393, CVE-2024-27395, CVE-2024-24858, CVE-2024-35912, CVE-2024-35847, CVE-2024-26960, CVE-2024-26961, CVE-2024-26931, CVE-2024-35888, CVE-2024-35978, CVE-2024-27437, CVE-2024-35973, CVE-2024-35950, CVE-2024-35872, CVE-2024-26966, CVE-2024-26969, CVE-2024-35819, CVE-2024-26811, CVE-2024-26973, CVE-2024-27059, CVE-2024-35849, CVE-2024-27019, CVE-2024-35855, CVE-2024-35969, CVE-2024-27004, CVE-2024-26999, CVE-2024-35901, CVE-2024-26923, CVE-2024-26957, CVE-2024-35877, CVE-2024-35988, CVE-2024-27396, CVE-2024-35806, CVE-2024-26951, CVE-2024-35927, CVE-2024-35898, CVE-2024-35895, CVE-2024-35809, CVE-2024-35854, CVE-2024-24859, CVE-2024-26687, CVE-2024-35934, CVE-2024-36005, CVE-2024-26965, CVE-2024-35821, CVE-2024-35896, CVE-2024-26993, CVE-2024-26817, CVE-2024-26984, CVE-2024-36029, CVE-2024-35825, CVE-2024-35960, CVE-2024-35851, CVE-2024-35925, CVE-2022-38096, CVE-2024-36007, CVE-2024-26956, CVE-2024-26981, CVE-2024-35897, CVE-2024-35997, CVE-2024-26934, CVE-2024-35984, CVE-2024-35871, CVE-2024-27001, CVE-2024-23307, CVE-2024-35805, CVE-2024-26813, CVE-2023-52880, CVE-2024-26814, CVE-2024-35936, CVE-2024-35886, CVE-2024-35915, CVE-2024-26988, CVE-2024-35807, CVE-2024-35902, CVE-2024-26654, CVE-2024-35884, CVE-2024-26970, CVE-2024-35982, CVE-2024-35958, CVE-2024-36025, CVE-2024-26989, CVE-2024-35817, CVE-2024-26929, CVE-2024-35905, CVE-2024-27008)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Denial of Service, NULL Pointer Dereference, Integer Overflow, Race Condition. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 22.04 Ubuntu 20.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6898-1

Affected Product	**HPE**
Severity	**Medium**
Affected Vulnerability	Multiple Denial of Service Vulnerabilities (CVE-2024-0727, CVE-2023-5678)
Description	HPE has released security updates addressing multiple Denial of Service vulnerabilities that exist in HPE ProLiant DL/ML/XL, Synergy, Edgeline and Alletra Servers. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE ProLiant DL20 Gen11 -Prior to v1.48_03-14-2024 HPE ProLiant DL110 Gen11 -Prior to v2.20_05-27-2024 HPE ProLiant DL320 Gen11 Server -Prior to v2.20_05-27-2024 HPE ProLiant DL360 Gen11 Server -Prior to v2.20_05-27-2024 HPE ProLiant DL380 Gen11 Server -Prior to v2.20_05-27-2024 HPE ProLiant DL380a Gen11 -Prior to v2.20_05-27-2024 HPE ProLiant DL560 Gen11 -Prior to v2.20_05-27-2024 HPE ProLiant MicroServer Gen11 -Prior to v1.48_03-14-2024 HPE ProLiant ML30 Gen11 -Prior to v1.48_03-14-2024 HPE ProLiant ML110 Gen11 -Prior to v2.20_05-27-2024 HPE ProLiant ML350 Gen11 Server -Prior to v2.20_05-27-2024 HPE ProLiant DL20 Gen10 Plus server -Prior to v2.10_05-16-2024 HPE ProLiant DL110 Gen10 Plus Telco server -Prior to v2.10_05-16-2024 HPE ProLiant DL360 Gen10 Plus server -Prior to v2.10_05-16-2024 HPE ProLiant DL380 Gen10 Plus server -Prior to v2.10_05-16-2024 HPE ProLiant ML30 Gen10 Plus server -Prior to v2.10_05-16-2024 HPE ProLiant MicroServer Gen10 Plus -Prior to v3.10_05-16-2024 HPE ProLiant MicroServer Gen10 Plus v2 -Prior to v2.10_05-16-2024 HPE Alletra 4110 -Prior to v2.20_05-27-2024 HPE Alletra 4120 -Prior to v2.20_05-27-2024 HPE ProLiant ML30 Gen10 Server -Prior to v3.10_05-16-2024 HPE ProLiant DL20 Gen10 Server -Prior to v3.10_05-16-2024 HPE ProLiant DL360 Gen10 Server -Prior to v3.20_05-27-2024 HPE ProLiant DL160 Gen10 Server -Prior to v3.20_05-27-2024 HPE ProLiant DL180 Gen10 Server -Prior to v3.20_05-27-2024 HPE ProLiant DL380 Gen10 Server -Prior to v3.20_05-27-2024 HPE ProLiant DL560 Gen10 Server -Prior to v3.20_05-27-2024 HPE ProLiant ML110 Gen10 Server -Prior to v3.20_05-27-2024 HPE ProLiant ML350 Gen10 Server -Prior to v3.20_05-27-2024 HPE ProLiant MicroServer Gen10 -Prior to v3.10_05-16-2024 HPE Synergy 480 Gen11 Compute Module -Prior to v2.20_05-27-2024 HPE Synergy 480 Gen10 Plus Compute Module -Prior to v2.10_05-27-2024 HPE ProLiant BL460c Gen10 Server Blade -Prior to v3.20_05-27-2024 HPE Synergy 480 Gen10 Compute Module -Prior to v3.20_05-27-2024 HPE Synergy 660 Gen10 Compute Module -Prior to v3.20_05-27-2024 HPE ProLiant e910 Server Blade -Prior to v3.20_05-27-2024 HPE ProLiant e910t Server Blade -Prior to v3.20_05-27-2024 HPE Edgeline e920 Server Blade -Prior to v2.10_05-27-2024 HPE Edgeline e920d Server Blade -Prior to v2.10_05-27-2024 HPE Edgeline e920t Server Blade -Prior to v2.10_05-27-2024 HPE Compute Edge Server e930t -Prior to v2.20_05-27-2024 HPE ProLiant DL325 Gen11 Server -Prior to v1.60_03-21-2024 HPE ProLiant DL345 Gen11 Server -Prior to v1.60_03-21-2024 HPE ProLiant DL365 Gen11 Server -Prior to v1.60_03-21-2024 HPE ProLiant DL385 Gen11 Server -Prior to v1.60_03-21-2024 HPE ProLiant DL325 Gen10 Plus server -Prior to v3.10_05-16-2024 HPE ProLiant DL325 Gen10 Plus v2 server -Prior to v3.10_05-16-2024 HPE ProLiant DL345 Gen10 Plus server -Prior to v3.10_05-16-2024 HPE ProLiant DL365 Gen10 Plus server -Prior to v3.10_05-16-2024 HPE ProLiant DL385 Gen10 Plus server -Prior to v3.10_05-16-2024 HPE ProLiant DL385 Gen10 Plus v2 server -Prior to v3.10_05-16-2024 HPE ProLiant DL325 Gen10 Server -Prior to v3.10_05-16-2024 HPE ProLiant DL385 Gen10 Server -Prior to v3.10_05-16-2024 HPE ProLiant XL645d Gen10 Plus Server -Prior to v3.10_05-17-2024 HPE ProLiant XL675d Gen10 Plus Server -Prior to v3.10_05-17-2024 HPE Apollo 2000 Gen10 Plus System -Prior to v2.10_05-27-2024 HPE Apollo 4200 Gen10 Plus System -Prior to v2.10_05-27-2024 HPE ProLiant XL220n Gen10 Plus Server -Prior to v2.10_05-27-2024 HPE ProLiant XL290n Gen10 Plus Server -Prior to v2.10_05-27-2024 HPE ProLiant XL170r Gen10 Server -Prior to v3.20_05-27-2024 HPE ProLiant XL190r Gen10 Server -Prior to v3.20_05-27-2024
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04603en_us&docLocale=en_US

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-22081, CVE-2023-22067, CVE-2023-5676)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2023-22081 -** An unspecified vulnerability in Java SE related to the JSSE component could allow a remote attacker to cause no confidentiality impact, no integrity impact, and low availability impact. **CVE-2023-22067 -** An unspecified vulnerability in Java SE related to the CORBA component could allow a remote attacker to cause no confidentiality impact, low integrity impact, and no availability impact. **CVE-2023-5676 -** Eclipse OpenJ9 is vulnerable to a denial of service, caused by a flaw when a shutdown signal (SIGTERM, SIGINT or SIGHUP) is received before the JVM has finished initializing. By sending a specially crafted request, a local authenticated attacker could exploit this vulnerability to cause an infinite busy hang on a spinlock or a segmentation fault. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Protect Operations Center - Version 8.1 IBM Storage Protect Server - Version 8.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7144627 • https://www.ibm.com/support/pages/node/7160302

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.