Advisory Alert

Alert Number: **AAA20240403** **Date:** **April 3, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HPE	**High**	Multiple Vulnerabilities
Dell	**High**	Improper Privilege Management Security Vulnerability
VMware	**High**	Multiple Vulnerabilities
Red Hat	**High**, **Medium**	Multiple Vulnerabilities
IBM	**High**, **Medium**	Multiple Vulnerabilities

Description

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-22437, CVE-2021-38575, CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, CVE-2023-45237)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in HPE MSA storage products and HPE ProLiant Servers. Exploitation of these vulnerabilities could lead to Remote code execution, Denial of service, Information disclosure and Local unauthorized access. HPE recommends to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE MSA 1040 SAN Storage - Prior to v4.1.3.83 HPE MSA 1050 SAN Storage - Prior to v4.1.3.83 HPE MSA 1060 Storage - Prior to v4.1.3.83 HPE MSA 2040 SAN Storage - Prior to v4.1.3.83 HPE MSA 2042 SAN Storage - Prior to v4.1.3.83 HPE MSA 2050 SAN Storage - Prior to v4.1.3.83 HPE MSA 2052 SAN Storage - Prior to v4.1.3.83 HPE MSA 2060 Storage - Prior to v4.1.3.83 HPE MSA 2062 Storage - Prior to v4.1.3.83 HPE ProLiant DL110 Gen11 - Prior to v2.16_03-01-2024 HPE ProLiant DL320 Gen11 Server - Prior to v2.16_03-01-2024 HPE ProLiant DL360 Gen11 Server - Prior to v2.16_03-01-2024 HPE ProLiant DL380 Gen11 Server - Prior to v2.16_03-01-2024 HPE ProLiant DL380a Gen11 - Prior to v2.16_03-01-2024 HPE ProLiant DL560 Gen11 - Prior to v2.16_03-01-2024 HPE ProLiant ML110 Gen11 - Prior to v2.16_03-01-2024 HPE ProLiant ML350 Gen11 Server - Prior to v2.16_03-01-2024 HPE Alletra 4110 - Prior to v2.16_03-01-2024 HPE Alletra 4120 - Prior to v2.16_03-01-2024 HPE ProLiant DL110 Gen10 Plus Telco server - Prior to v2.00_02-22-2024 HPE ProLiant DL360 Gen10 Plus server - Prior to v2.00_03-06-2024 HPE ProLiant DL380 Gen10 Plus server - Prior to v2.00_03-06-2024 HPE ProLiant DL160 Gen10 Server - Prior to v3.10_02-22-2024 HPE ProLiant DL180 Gen10 Server - Prior to v3.10_02-22-2024 HPE ProLiant DL360 Gen10 Server - Prior to v3.10_02-22-2024 HPE ProLiant DL380 Gen10 Server - Prior to v3.10_02-22-2024 HPE ProLiant DL560 Gen10 Server - Prior to v3.10_02-22-2024 HPE ProLiant ML110 Gen10 Server - Prior to v3.10_02-22-2024 HPE ProLiant ML350 Gen10 Server - Prior to v3.10_02-22-2024 HPE Synergy 480 Gen11 Compute Module - Prior to v2.16_03-01-2024 HPE Synergy 480 Gen10 Plus Compute Module - Prior to v2.00_02-22-2024 HPE ProLiant BL460c Gen10 Server Blade - Prior to v3.10_02-22-2024 HPE Synergy 480 Gen10 Compute Module - Prior to v3.10_02-22-2024 HPE Synergy 660 Gen10 Compute Module - Prior to v3.10_02-22-2024 HPE Apollo 4200 Gen10 Plus System - Prior to v2.00_02-22-2024 HPE ProLiant XL220n Gen10 Plus Server - Prior to v2.00_02-22-2024 HPE ProLiant XL290n Gen10 Plus Server - Prior to v2.00_02-22-2024 HPE Apollo 2000 Gen10 Plus System - Prior to v2.00_02-22-2024 HPE Apollo 2000 System - Prior to v3.10_02-22-2024 HPE ProLiant e910 Server Blade - Prior to v3.10_02-22-2024 HPE ProLiant e910t Server Blade - Prior to v3.10_02-22-2024 HPE Edgeline e920 Server Blade - Prior to v2.00_02-22-2024 HPE Edgeline e920d Server Blade - Prior to v2.00_02-22-2024 HPE Edgeline e920t Server Blade - Prior to v2.00_02-22-2024 HPE Compute Edge Server e930t - Prior to v2.16_03-01-2024 HPE ProLiant XL225n Gen10 Plus 1U Node - Prior to v3.00_01-26-2024 HPE ProLiant RL300 Gen11 - Prior to v1.60_03-07-2024
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbst04630en_us • https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04593en_us

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Improper Privilege Management Security Vulnerability (CVE-2024-0172)
Description	Dell has released security updates addressing Improper privilege management security vulnerability that exists in their Dell PowerEdge Servers and Dell EMC Storage Devices. Exploitation of these vulnerabilities could lead to compromise the affected system. Dell recommends to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Dell Devices
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000223727/dsa-2024-035-security-update-for-dell-poweredge-server-bios-for-an-improper-privilege-management-security-vulnerability

Affected Product	**VMware**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-22246, CVE-2024-22247, CVE-2024-22248)
Description	VMware has released security updates addressing multiple vulnerabilities that exist in their VMware SD-WAN products. Exploitation of these vulnerabilities could lead to Remote code execution and command Injection to the router. VMware recommends to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	VMware SD-WAN (Edge) - Versions 4.5.x/5.x VMware SD-WAN (Orchestrator) - Versions 5.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2024-0008.html

Affected Product	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-33631, CVE-2022-38096, CVE-2023-6546, CVE-2023-6931, CVE-2023-51042, CVE-2024-0565, CVE-2024-1086, CVE-2023-1118, CVE-2024-26602)
Description	Red Hat has released security updates addressing vulnerabilities that exist in their products. Exploitation of these vulnerabilities could lead to Use-after-free, Privilege escalation, NULL pointer dereference and Remote Code Execution. Red Hat recommends to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux for IBM z Systems 8 s390x Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for ARM 64 8 aarch64 Red Hat CodeReady Linux Builder for x86_64 8 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le Red Hat CodeReady Linux Builder for ARM 64 8 aarch64 Red Hat Enterprise Linux for Real Time 8 x86_64 Red Hat Enterprise Linux for Real Time for NFV 8 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.6 x86_64 Red Hat Enterprise Linux Server - AUS 8.6 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.6 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.6 ppc64le Red Hat Virtualization Host 4 for RHEL 8 x86_64 Red Hat Enterprise Linux Server - TUS 8.6 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.6 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 8.6 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 8.6 ppc64le Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 8.6 aarch64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2024:1607 • https://access.redhat.com/errata/RHSA-2024:1612 • https://access.redhat.com/errata/RHSA-2024:1614 • https://access.redhat.com/errata/RHSA-2024:1653 • https://access.redhat.com/errata/RHSA-2024:1612

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-22360, CVE-2024-27254, CVE-2024-25046, CVE-2024-25030, CVE-2012-2677, CVE-2023-52296, CVE-2023-38729, CVE-2024-28782)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities could lead to Denial of service, Execute arbitrary code, Information disclosure. IBM recommends to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Db2 - Versions 11.5.x IBM Db2 - Versions 10.5.0.x IBM Db2 - Versions 11.1.4.x IBM Cloud Pak for Security - Versions 1.10.0.0 - 1.10.11.0 QRadar Suite Software - Versions 1.10.12.0 - 1.10.18.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7145730 • https://www.ibm.com/support/pages/node/7145727 • https://www.ibm.com/support/pages/node/7145726 • https://www.ibm.com/support/pages/node/7145725 • https://www.ibm.com/support/pages/node/7145724 • https://www.ibm.com/support/pages/node/7145722 • https://www.ibm.com/support/pages/node/7145721 • https://www.ibm.com/support/pages/node/7145683

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.