Advisory Alert

Alert Number: **AAA20250205** **Date:** **February 5, 2025**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Veeam	**Critical**	Arbitrary Code Execution Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Multiple Vulnerabilities
Dell	**High**	AMD Confidential Computing Vulnerability
Ubuntu	**High, Medium**	Multiple Vulnerabilities
HPE	**High, Medium**	Multiple Vulnerabilities
IBM	**High, Medium, Low**	Multiple Vulnerabilities
MariaDB	**Medium**	Security Update

Description

Affected Product	**Veeam**
Severity	**Critical**
Affected Vulnerability	Arbitrary Code Execution Vulnerability (CVE-2025-23114)
Description	Veeam has released a security update addressing an Arbitrary Code Execution Vulnerability in their products. **CVE-2025-23114 -** A vulnerability within the Veeam Updater component that allows an attacker to utilize a Man-in-the-Middle attack to execute arbitrary code on the affected appliance server with root-level permissions. Veeam advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Veeam Backup for Salesforce - 3.1 and older
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.veeam.com/kb4712

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released a security update addressing multiple vulnerabilities in third-party products, which, in turn, affect Dell VxRail. If exploited, malicious users could compromise the affected system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell VxRail Appliance - Versions 8.0.000 through 8.0.320
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000280531/dsa-2025-065-security-update-for-dell-vxrail-for-multiple-third-party-component-vulnerabilities

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. If exploited these vulnerabilities could cause denial of services, information disclosure, arbitrary code execution. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Security QRadar EDR - 3.12 IBM Cloud Pak for Security - 1.10.0.0 - 1.10.11.0 QRadar Suite Software - 1.10.12.0 - 1.10.24.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7182424 • https://www.ibm.com/support/pages/node/7167599

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	AMD Confidential Computing Vulnerability (CVE-2024-56161)
Description	Dell has released a security update addressing an AMD Confidential Computing Vulnerability in third-party products, which, in turn, affect Dell AMD-based PowerEdge Servers. If exploited, malicious users could compromise the affected system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell PowerEdge R6615 BIOS Versions prior to 1.11.2 Dell PowerEdge R7615 BIOS Versions prior to 1.11.2 Dell PowerEdge R6625 BIOS Versions prior to 1.11.2 Dell PowerEdge R7625 BIOS Versions prior to 1.11.2 Dell PowerEdge C6615 BIOS Versions prior to 1.6.2 Dell XC Core XC7625 BIOS Versions prior to 1.11.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000280550/dsa-2025-040-security-update-for-dell-amd-based-poweredge-server-vulnerabilities

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-53164, CVE-2024-53103)
Description	Ubuntu has released security updates to address multiple vulnerabilities in their products. **CVE-2024-53164 -** In the Linux kernel, the following vulnerability has been resolved: net: sched: fix ordering of qlen adjustment Changes to sch->q.qlen around qdisc_tree_reduce_backlog() need to happen _before_ a call to said function because otherwise it may fail to notify parent qdiscs when the child is about to become empty. **CVE-2024-53103 -** In the Linux kernel, the following vulnerability has been resolved: hv_sock: Initializing vsk->trans to NULL to prevent a dangling pointer When hvs is released, there is a possibility that vsk->trans may not be initialized to NULL, which could lead to a dangling pointer. This issue is resolved by initializing vsk->trans to NULL. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 24.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-7238-3

Affected Product	**HPE**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-56161, CVE-2024-21944, CVE-2025-25039, CVE-2025-23060, CVE-2025-23059, CVE-2025-23058, CVE-2024-7348, CVE-2024-24980, CVE-2024-24853)
Description	HPE has released security updates addressing multiple vulnerabilities in their products. If exploited, these vulnerabilities could lead to unauthorized access, compromise of system integrity, arbitrary code execution, escalation of privilege. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Aruba Networking ClearPass Policy Manager, • 6.12.x: 6.12.3 and below • 6.11.x: 6.11.9 and below HPE ProLiant DL145 Gen11 - Prior to v1.40 HPE ProLiant DL325 Gen10 Plus server - Prior to v3.60_01-16-2025 HPE ProLiant DL325 Gen10 Plus v2 server - Prior to v3.60, Prior to v3.60_01-16-2025 HPE ProLiant DL325 Gen10 Server - Prior to v3.40_01-16-2025 HPE ProLiant DL325 Gen11 Server - Prior to v2.30, Prior to v2.30_01-17-2025 HPE ProLiant DL345 Gen10 Plus server - Prior to v3.60, Prior to v3.60_01-16-2025 HPE ProLiant DL345 Gen11 Server - Prior to v2.30, Prior to v2.30_01-17-2025 HPE ProLiant DL365 Gen10 Plus server - Prior to v3.60, Prior to v3.60_01-16-2025 HPE ProLiant DL365 Gen11 Server - Prior to v2.30, Prior to v2.30_01-17-2025 HPE ProLiant DL385 Gen10 Plus server - Prior to v3.60, Prior to v3.60_01-16-2025 HPE ProLiant DL385 Gen10 Plus v2 server - Prior to v3.60, Prior to v3.60_01-16-2025 HPE ProLiant DL385 Gen10 Server - Prior to v3.40_01-16-2025 HPE ProLiant DL385 Gen11 Server - Prior to v2.30, Prior to v2.30_01-17-2025 HPE ProLiant DX170r Gen10 server - Prior to v3.30_07-31-2024, Prior to v3.30_07-31-2024 HPE ProLiant DX220n Gen10 Plus server - Prior to v2.20_08-07-2024 HPE ProLiant DX360 Gen10 Plus server - Prior to v2.20_08-07-2024 HPE ProLiant DX360 Gen10 server - Prior to v3.30_07-31-2024 HPE ProLiant DX360 Gen11 - Prior to v2.20_05-27-2024 HPE ProLiant DX380 Gen10 Plus server - Prior to v2.20_08-07-2024 HPE ProLiant DX380 Gen10 server - Prior to v3.30_07-31-2024 HPE ProLiant DX380 Gen11 - Prior to v2.20_05-27-2024 HPE ProLiant DX4200 Gen10 server - Prior to v3.30_07-31-2024 HPE ProLiant DX560 Gen10 server - Prior to v3.30_07-31-2024 HPE ProLiant XL225n Gen10 Plus 1U Node - Prior to v3.60, Prior to v3.60_01-16-2025 HPE ProLiant XL645d Gen10 Plus Server - Prior to v3.60, Prior to v3.60_01-16-2025 HPE ProLiant XL675d Gen10 Plus Server - Prior to v3.60, Prior to v3.60_01-16-2025
Officially Acknowledged by the Vendor	Yes
`Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04774en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04783en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04784en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04779en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04781en_us&docLocale=en_US

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-26643, CVE-2024-27397, CVE-2024-22354, CVE-2023-6240, CVE-2023-52667, CVE-2024-33601, CVE-2024-22329, CVE-2023-52675, CVE-2024-26659, CVE-2024-26735, CVE-2024-25026, CVE-2024-26602, CVE-2024-33599, CVE-2023-52686, CVE-2024-36004, CVE-2023-52835, CVE-2024-26585, CVE-2024-33602, CVE-2024-26993, CVE-2024-33600, CVE-2024-6387, CVE-2024-26583, CVE-2024-26584, CVE-2023-4244, CVE-2024-0443, CVE-2024-26804, CVE-2024-26808, CVE-2024-2961, CVE-2023-45853, CVE-2023-29267, CVE-2024-25710, CVE-2024-26308, CVE-2023-45178, CVE-2024-28762, CVE-2024-28757, CVE-2024-29025, CVE-2024-29131, CVE-2024-29133, CVE-2024-31880, CVE-2024-31881, CVE-2023-45288, CVE-2024-21147, CVE-2024-21145, CVE-2024-21140, CVE-2024-21144, CVE-2024-21138, CVE-2024-21131, CVE-2024-27267, CVE-2024-26586, CVE-2024-26733, CVE-2024-27019, CVE-2023-52530, CVE-2024-27011, CVE-2024-26759, CVE-2024-26960, CVE-2024-37891, CVE-2024-5564, CVE-2023-2953, CVE-2023-31346, CVE-2024-25629, CVE-2020-26555, CVE-2021-46909, CVE-2021-46972, CVE-2021-47069, CVE-2021-47073, CVE-2021-47236, CVE-2021-47310, CVE-2021-47311, CVE-2021-47353, CVE-2021-47356, CVE-2021-47456, CVE-2021-47495, CVE-2023-5090, CVE-2023-52464, CVE-2023-52560, CVE-2023-52615, CVE-2023-52626, CVE-2023-52669, CVE-2023-52700, CVE-2023-52703, CVE-2023-52781, CVE-2023-52813, CVE-2023-52877, CVE-2023-52878, CVE-2023-52881, CVE-2024-26656, CVE-2024-26675, CVE-2024-26801, CVE-2024-26826, CVE-2024-26859, CVE-2024-26906, CVE-2024-26907, CVE-2024-26974, CVE-2024-26982, CVE-2024-27410, CVE-2024-35789, CVE-2024-35835, CVE-2024-35838, CVE-2024-35845, CVE-2024-35852, CVE-2024-35853, CVE-2024-35854, CVE-2024-35855, CVE-2024-35888, CVE-2024-35890, CVE-2024-35958, CVE-2024-35959, CVE-2024-35960, CVE-2024-36007, CVE-2022-48624, CVE-2024-32487, CVE-2024-3651, CVE-2024-28182, CVE-2024-6345, CVE-2024-37890, CVE-2024-39689, CVE-2024-34069, CVE-2024-35195)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. If exploited these vulnerabilities could cause denial of services, information disclosure, arbitrary code execution, server-side request forgery (SSRF). IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Scale System 6.1.0.0-6.1.9.3 - 6.2.0.0-6.2.0.1 IBM Storage Protect Server - 8.1 IBM Storage Insights - Data Collector - 20250101-0914 IBM Storage Copy Data Management - 2.2.0.0 - 2.2.24.0 IBM QRadar Network Packet Capture - 7.5.0 - 7.5.0 Update Package 9 IBM Cloud Pak for Security - 1.10.0.0 - 1.10.11.0 QRadar Suite Software - 1.10.12.0 - 1.10.24.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7173184 • https://www.ibm.com/support/pages/node/7173226 • https://www.ibm.com/support/pages/node/7173201 • https://www.ibm.com/support/pages/node/7182409 • https://www.ibm.com/support/pages/node/7168681 • https://www.ibm.com/support/pages/node/7173421 • https://www.ibm.com/support/pages/node/7167599

Affected Product	**MariaDB**
Severity	**Medium**
Affected Vulnerability	Security Update (CVE-2025-21490)
Description	MariaDB has released security updates to address a vulnerability in third-party products, which, in turn, affect their products. If exploited, malicious users could compromise the affected system. MariaDB advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	MariaDB 11.4.5 MariaDB 10.6.21 MariaDB 10.5.28 MariaDB 10.11.11
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://mariadb.com/kb/en/mariadb-11-4-5-release-notes/ • https://mariadb.com/kb/en/mariadb-10-6-21-release-notes/ • https://mariadb.com/kb/en/mariadb-10-5-28-release-notes/ • https://mariadb.com/kb/en/mariadb-10-11-11-release-notes/

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.