Advisory Alert

Alert Number: AAA20250521 **Date:** May 21, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Authorization Bypass Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
Broadcom VMware	**High**, Medium	Multiple Vulnerabilities
IBM	**High**, Medium, Low	Multiple Vulnerabilities

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Authorization Bypass Vulnerability (CVE-2024-45337)
Description	IBM has released a security update addressing an Authorization Bypass Vulnerability in IBM Security QRadar EDR. **CVE-2024-45337** - Applications and libraries which misuse connection.serverAuthenticate (via callback field ServerConfig.PublicKeyCallback) may be susceptible to an authorization bypass. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Security QRadar EDR 3.12
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7234028

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-21756, CVE-2024-40906, CVE-2024-44970)
Description	Red Hat has released a security update addressing multiple vulnerabilities in their products. **CVE-2025-21756 -** A flaw was found in the Linux kernel's VMware network driver, where an improperly timed socket unbinding could result in a use-after-free issue. This flaw allows an attacker who can create and destroy arbitrary connections on virtual connections to read or modify system memory, potentially leading to an escalation of privileges or the compromise of sensitive data. **CVE-2024-44970 -** net/mlx5e: SHAMPO, Fix invalid WQ linked list unlink When all the strides in a WQE have been consumed, the WQE is unlinked from the WQ linked list (mlx5_wq_ll_pop()). For SHAMPO, it is possible to receive CQEs with 0 consumed strides for the same WQE even after the WQE is fully consumed and unlinked. This triggers an additional unlink for the same wqe which corrupts the linked list. Fix this scenario by accepting 0 sized consumed strides without unlinking the WQE again. **CVE-2024-40906 -** net/mlx5: Always stop health timer during driver removal Currently, if teardown_hca fails to execute during driver removal, mlx5 does not stop the health timer. Afterwards, mlx5 continue with driver teardown. This may lead to a UAF bug, which results in page fault Oops[1], since the health timer invokes after resources were freed. Hence, stop the health monitor even if teardown_hca fails**.** Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat CodeReady Linux Builder for ARM 64 8 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.4 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 8 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.4 x86_64 Red Hat CodeReady Linux Builder for x86_64 8 x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat Enterprise Linux for ARM 64 8 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.4 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x Red Hat Enterprise Linux for IBM z Systems 8 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat Enterprise Linux for Power, little endian 8 ppc64le 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 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 8 x86_64 Red Hat Enterprise Linux Server - AUS 9.4 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:8058 • https://access.redhat.com/errata/RHSA-2025:8057 • https://access.redhat.com/errata/RHSA-2025:8056

Affected Product	**Broadcom VMware**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-41225, CVE-2025-41226, CVE-2025-41227, CVE-2025-41228, CVE-2025-41229, CVE-2025-41230, CVE-2025-41231)
Description	Broadcom has released a security update addressing multiple vulnerabilities in VMware. If exploited these vulnerabilities could lead to Directory Traversal, Information Disclosure, arbitrary commands execution, Denial-of-Service. Broadcom advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	vCenter Server 7.0 vCenter Server 8.0 VMware Cloud Foundation 4.5.x and 5.x VMware Cloud Foundation (ESXi) 4.5.x VMware Cloud Foundation (ESXi) 5.x VMware Cloud Foundation (vCenter) 4.5.x VMware Cloud Foundation (vCenter) 5.x VMware ESXi 7.0 VMware ESXi 8.0 VMware Fusion 13.x VMware Telco Cloud Infrastructure (ESXi) 2.x VMware Telco Cloud Infrastructure (ESXi) 3.x VMware Telco Cloud Infrastructure (vCenter) 2.x VMware Telco Cloud Infrastructure (vCenter) 3.x VMware Telco Cloud Platform (ESXi) 5.x, 4.x, 3.x, 2.x VMware Telco Cloud Platform (vCenter) 5.x, 4.x, 3.x, 2.x VMware Workstation 17.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/security-advisories/0/25733 • https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/security-advisories/0/25717

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-8176, CVE-2024-45641, CVE-2023-33861, CVE-2025-22869, CVE-2025-22870, CVE-2025-27363, CVE-2024-12797, CVE-2025-27152, CVE-2024-12705, CVE-2024-11187)
Description	IBM has released security updates addressing multiple vulnerabilities in their products. These vulnerabilities could be exploited by malicious users to cause denial of service, credential leakage, arbitrary code execution, memory corruption. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Security QRadar EDR 3.12 AIX 7.3 , 7.2 VIOS 4.1 , 3.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7233972 • https://www.ibm.com/support/pages/node/7234028 • https://www.ibm.com/support/pages/node/7233972 • https://www.ibm.com/support/pages/node/7233966 • https://www.ibm.com/support/pages/node/7233964

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.