Advisory Alert

Alert Number: AAA20250930 **Date:** September 30, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Broadcom VMware	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
F5	**High**, Medium	Multiple Vulnerabilities
Red Hat	Medium	Multiple Vulnerabilities

Description

Affected Product	**Broadcom VMware**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-41244,CVE-2025-41245, CVE-2025-41246, CVE-2025-41250, CVE-2025-41251, CVE-2025-41252)
Description	Broadcom has released security updates addressing multiple vulnerabilities that exist in VMware products. These vulnerabilities could be exploited by malicious users to cause Local Privilege Escalation, Information Disclosure, Brute-force attacks, unauthorized access. Broadcom advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	VMware Aria Operations versions prior to 8.18.5 VMware Tools 12.x.x and 11.x.x - versions prior to 12.5.4 VMware Tools 13.x.x - versions prior to 13.0.5 VMware vCenter 8.0 - versions prior to 8.0 U3g VMware vCenter 7.0 - versions prior to 7.0 U3w VMware NSX 4.2.x - versions prior to 4.2.2.2 and prior to 4.2.3.1 VMware NSX 4.1.x and 4.0.x - versions prior to 4.1.2.7 NSX-T 3.x - versions prior to 3.2.4.3 VMware Cloud Foundation/ VMware vSphere Foundation - Operations versions prior to 9.0.1.0 VMware Cloud Foundation/ VMware vSphere Foundation - VMware Tools versions prior to 13.0.5.0 VMware Cloud Foundation/ VMware vSphere Foundation - VMware NSX versions prior to 9.0.1.0 VMware Cloud Foundation 5.x and 4.x - versions prior to KB92148 VMware Cloud Foundation vCenter 5.x - versions prior to 5.2.2 VMware Cloud Foundation vCenter 4.5.x - versions prior to Async patch - 7.0 U3w VMware Cloud Foundation - VMware NSX 5.x - versions prior to KB88287 VMware Cloud Foundation - VMware NSX 4.5.x - versions prior to KB88287 VMware Telco Cloud Platform - VMware Aria Operations 5.x and 4.x - versions prior to 8.18.5 VMware Telco Cloud Platform - vCenter 5.x, 4.x, 3.x, 2.x - versions prior to KB411508 VMware Telco Cloud Platform - VMware NSX 5.x, 4.x, 3.x - versions prior to KB411518 VMware Telco Cloud Infrastructure - vCenter 3.x, 2.x - versions prior to KB411508 VMware Telco Cloud Infrastructure - VMware NSX 3.x and 2.x - versions prior to KB411518 VMware Telco Cloud Infrastructure - VMware Aria Operations 3.x and 2.x versions prior to 8.18.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36149 • https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36150

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-20613, CVE-2025-22853, CVE-2025-21096, CVE-2025-20053, CVE-2025-21090, CVE-2025-24305)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in Intel TDX Module and Intel Xeon Processor Firmware Cache which affect Dell Precision Rack BIOS. 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	Precision 7960 Rack BIOS Versions prior to 2.7.5 Precision 7960 XL Rack BIOS Versions prior to 2.7.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000373803/dsa-2025-372

Affected Product	**F5**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2018-10103, CVE-2018-10105)
Description	F5 has released security updates addressing multiple vulnerabilities that exist in tcpdump which affects F5 products. **CVE-2018-10103/ CVE-2018-10105** - tcpdump before 4.9.3 mishandles the printing of SMB data. These vulnerabilities can result in denial of service (DoS) or, potentially, execution of arbitrary code. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP (all modules) versions 15.0.0 - 15.1.2 BIG-IQ Centralized Management versions 8.3.0 - 8.4.0 F5OS-A versions 1.8.0 and 1.5.1 - 1.5.3 F5OS-C versions 1.8.0 - 1.8.1 and 1.6.0 - 1.6.2 Traffix SDC versions 5.0.0 - 5.2.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000156675

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-22058, CVE-2025-22097, CVE-2025-38477, CVE-2025-38396, CVE-2025-38523, CVE-2025-38527, CVE-2025-39682, CVE-2025-39694, CVE-2025-39698)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. 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 10.0 aarch64 Red Hat CodeReady Linux Builder for ARM 64 10 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 10.0 s390x Red Hat CodeReady Linux Builder for IBM z Systems 10 s390x Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 10.0 ppc64le Red Hat CodeReady Linux Builder for Power, little endian 10 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 10.0 x86_64 Red Hat CodeReady Linux Builder for x86_64 10 x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 10.0 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 10.0 aarch64 Red Hat Enterprise Linux for ARM 64 10 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 10.0 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 10.0 s390x Red Hat Enterprise Linux for IBM z Systems 10 s390x Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.0 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 10.0 ppc64le Red Hat Enterprise Linux for Power, little endian 10 ppc64le Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.0 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 10.0 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.8 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.8 x86_64 Red Hat Enterprise Linux for x86_64 10 x86_64 Red Hat Enterprise Linux Server - TUS 8.8 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.8 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:17009 • https://access.redhat.com/errata/RHSA-2025:16904

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.