Advisory Alert

Alert Number: AAA20240527 **Date:** May 27, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**High**	Multiple Vulnerabilities
Red Hat	**High**, **Medium**	Multiple Vulnerabilities
F5	**High**, **Medium**	Multiple Vulnerabilities
Ubuntu	**Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell 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. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell EMC VxRail Appliance - 7.0.x versions prior to 7.0.484
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000225327/dsa-2024-215-security-update-for-dell-vxrail-7-0-484-multiple-third-party-component-vulnerabilities

Affected Product	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-40982, CVE-2024-1086, CVE-2024-26642, CVE-2024-26643, CVE-2024-26673, CVE-2024-26804, CVE-2019-13631, CVE-2019-15505, CVE-2020-25656, CVE-2021-3753, CVE-2021-4204, CVE-2022-0500, CVE-2022-3565, CVE-2022-23222, CVE-2022-45934, CVE-2023-1513, CVE-2023-3567, CVE-2023-4133, CVE-2023-4244, CVE-2023-6121, CVE-2023-6176, CVE-2023-6622, CVE-2023-6915, CVE-2023-6932, CVE-2023-24023, CVE-2023-25775, CVE-2023-28464, CVE-2023-31083, CVE-2023-37453, CVE-2023-38409, CVE-2023-39189, CVE-2023-39192, CVE-2023-39193, CVE-2023-39194, CVE-2023-39198, CVE-2023-42754, CVE-2023-42755, CVE-2023-45863, CVE-2023-51779, CVE-2023-51780, CVE-2023-52340, CVE-2023-52434, CVE-2023-52448, CVE-2023-52489, CVE-2023-52574, CVE-2023-52580, CVE-2023-52581, CVE-2023-52620, CVE-2024-0841, CVE-2024-25742, CVE-2024-25743, CVE-2024-26602, CVE-2024-26609, CVE-2024-26671, CVE-2023-45288, CVE-2024-2494)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Privilege Escalation, Use After Free, NULL Pointer Dereference, Out of Bounds Read. 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, ARM 64 9 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.4 s390x Red Hat CodeReady Linux Builder for IBM z Systems 8 s390x, z Systems 9 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, little endian 9 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, x86_64 9 x86_64 Red Hat Container Native Virtualization 4.13 for RHEL 9 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat Enterprise Linux for ARM 64 8 aarch64, ARM 64 9 aarch64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x Red Hat Enterprise Linux for IBM z Systems 8 s390x, z Systems 9 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, little endian 9 ppc64le Red Hat Enterprise Linux for Real Time 9 x86_64 Red Hat Enterprise Linux for Real Time for NFV 9 x86_64 Red Hat Enterprise Linux for Real Time for NFV for x86_64 - 4 years of updates 9.4 x86_64 Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.4 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, x86_64 9 x86_64 Red Hat Enterprise Linux Server - AUS 7.6 x86_64, AUS 7.7 x86_64, AUS 9.4 x86_64 Red Hat Enterprise Linux Server for ARM 64 - 4 years of updates 9.4 aarch64 Red Hat Enterprise Linux Server for IBM z Systems - 4 years of updates 9.4 s390x 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-2024:3319 • https://access.redhat.com/errata/RHSA-2024:3318 • https://access.redhat.com/errata/RHSA-2024:3306 • https://access.redhat.com/errata/RHSA-2024:3138 • https://access.redhat.com/errata/RHSA-2024:3315 • https://access.redhat.com/errata/RHSA-2024:3253

Affected Product	**F5**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-38709, CVE-2022-43680)
Description	F5 has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2023-38709** - Faulty input validation in the core of Apache allows malicious or exploitable backend/content generators to split HTTP responses. **CVE-2022-43680** - In libexpat through 2.4.9, there is a use-after free caused by overeager destruction of a shared DTD in XML_ExternalEntityParserCreate in out-of-memory situations. F5 advises to apply security fixes at your earliest to protect systems from potential threats
Affected Products	BIG-IP (All Modules) – Version(s) 17.1.0 - 17.1.1 BIG-IP (All Modules) – Version(s) 16.1.0 - 16.1.4 BIG-IP (All Modules) – Version(s) 15.1.0 - 15.1.10 F5OS-A - Version(s) 1.7.0 / 1.5.1 - 1.5.2 F5OS-C - Version(s) 1.6.0 - 1.6.2 Traffix SDC - Version(s) 5.2.0 / 5.1.0 BIG-IQ Centralized Management - Version(s) 8.1.0 - 8.3.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://my.f5.com/manage/s/article/K000139525 • https://my.f5.com/manage/s/article/K000139764

Affected Product	**Ubuntu**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-26635, CVE-2021-46981, CVE-2023-52566, CVE-2023-52602 CVE-2024-26735, CVE-2024-26614, CVE-2024-26622, CVE-2023-52439, CVE-2023-52524 , CVE-2024-26801, CVE-2024-26704, CVE-2024-26805, CVE-2023-52604, CVE-2023-52530, CVE-2023-52601, CVE-2023-52583, CVE-2023-47233)
Description	Ubuntu 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. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 16.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6777-4

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.