Advisory Alert

Alert Number: AAA20250820 **Date:** August 20, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Oracle	**Critical**	Security Update
SUSE	**High**	Multiple Vulnerabilities
Commvault	**High**, Medium	Multiple Vulnerabilities
NetApp	**High**, Medium	Multiple Vulnerabilities
HPE	**High**, Medium	Multiple Vulnerabilities
Dell	**High**, Medium	Multiple Vulnerabilities
Ubuntu	**High**, Medium	Linux kernel vulnerabilities
Red Hat	**High**, Medium	Multiple Vulnerabilities
Oracle	**High**, Medium, Low	Multiple Vulnerabilities
IBM	Low	Security Restrictions Bypass Vulnerability

Description

Affected Product	**Oracle**
Severity	**Critical**
Affected Vulnerability	Security Update (CVE-2025-49794)
Description	Oracle has released monthly security update addressing a security vulnerability that exists in their product. These vulnerabilities could be exploited by malicious users to compromise the affected system. Oracle advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Oracle Solaris 11.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.oracle.com/security-alerts/bulletinjul2025.html

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE 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. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/

Affected Product	**Commvault**
Severity	**High**, Medium
Affected Vulnerability	Multiple Vulnerabilities
Description	Commvault has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause remote code execution, gain admin control, privilege escalation. Commvault advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Commvault Linux, Windows Platforms Versions - 11.36.0 - 11.36.59 Commvault Linux, Windows Platforms Versions - 11.32.0 - 11.32.101
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://documentation.commvault.com/securityadvisories/CV_2025_08_1.html • https://documentation.commvault.com/securityadvisories/CV_2025_08_2.html • https://documentation.commvault.com/securityadvisories/CV_2025_08_3.html • https://documentation.commvault.com/securityadvisories/CV_2025_08_4.html

Affected Product	**NetApp**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-29857, CVE-2024-30172, CVE-2024-34447, CVE-2022-38752, CVE-2022-41854, CVE-2022-25857, CVE-2022-38749, CVE-2022-38750, CVE-2022-38751, CVE-2025-21587, CVE-2025-30698, CVE-2024-30171)
Description	NetApp has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause sensitive information disclosure, addition or modification of data, denial of service, unauthorized read/update/insert. NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	NetApp BlueXP SANtricity Storage Plugin for vCenter
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.netapp.com/advisory/ntap-20241206-0008 • https://security.netapp.com/advisory/ntap-20240614-0007 • https://security.netapp.com/advisory/ntap-20240315-0009 • https://security.netapp.com/advisory/ntap-20240315-0010 • https://security.netapp.com/advisory/ntap-20250502-0005 • https://security.netapp.com/advisory/ntap-20240614-0008

Affected Product	**HPE**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-20037, CVE-2025-20067, CVE-2025-22392, CVE-2025-22839, CVE-2025-22840, CVE-2025-48976, CVE-2025-48988)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause disclosure of information, escalation of privilege, disclosure of information, denial of service. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04915en_us&docLocale=en_US https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04934en_us&docLocale=en_US https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04933en_us&docLocale=en_US https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbmu04921en_us&docLocale=en_US

Affected Product	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-36348, CVE-2024-36349, CVE-2024-36350, CVE-2024-36357, CVE-2024-45332, CVE-2025-20629, CVE-2023-20599, CVE-2024-39286, CVE-2024-38796, CVE-2025-29988, CVE-2025-24296)
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	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000270384/dsa-2025-044 • https://www.dell.com/support/kbdoc/en-us/000283859/dsa-2025-088 • https://www.dell.com/support/kbdoc/en-us/000330918/dsa-2025-236 • https://www.dell.com/support/kbdoc/en-us/000355835/dsa-2025-310-security-update-for-dell-ax-system-for-azure-local-multiple-third-party-component-vulnerabilities

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Linux kernel vulnerabilities (CVE-2025-38083, CVE-2025-37797, CVE-2024-50073, CVE-2024-49950, CVE-2024-38541, CVE-2023-52975, CVE-2023-52757, CVE-2025-21871, CVE-2025-21870, CVE-2025-21869, CVE-2025-21868, CVE-2025-21867, CVE-2025-21866, CVE-2025-21864, CVE-2025-21863, CVE-2025-21862, CVE-2025-21861, CVE-2025-38079, CVE-2025-38078, CVE-2025-38077, CVE-2025-38075, CVE-2025-38072, CVE-2025-38068, CVE-2025-38066, CVE-2025-38065, CVE-2025-38061, CVE-2025-38058)
Description	Ubuntu has released security updates addressing multiple Linux kernel 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 18.04, 20.04, 22.04, 24.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-7701-1 • https://ubuntu.com/security/notices/USN-7703-1 • https://ubuntu.com/security/notices/USN-7704-1

Affected Product	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-38380, CVE-2025-38471, CVE-2022-50020, CVE-2022-50022, CVE-2022-50200, CVE-2025-21727, CVE-2025-21991, CVE-2025-22020, CVE-2025-37797, CVE-2025-38086)
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 Enterprise Linux Server - AUS 9.4 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.4 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.4 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.4 s390x Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.0 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:14082 • https://access.redhat.com/errata/RHSA-2025:14094

Affected Product	**Oracle**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-50059,CVE-2025-27613,CVE-2025-24032,CVE-2024-53920,CVE-2024-55549,CVE-2025-32462,CVE-2022-49737,CVE-2025-5283,CVE-2025-6965,CVE-2025-22874,CVE-2025-32049,CVE-2025-47947,CVE-2025-6424,CVE-2025-32914,CVE-2025-49175,CVE-2025-32050,CVE-2025-0620,CVE-2020-27748,CVE-2023-28746,CVE-2024-6602,CVE-2025-4969,CVE-2025-31176,CVE-2025-32414,CVE-2025-29088,CVE-2025-48432,CVE-2024-12243,CVE-2024-47081,CVE-2024-53427,CVE-2025-48976,CVE-2024-34397,CVE-2025-5278,CVE-2024-7531,CVE-2025-32364,CVE-2024-58249,CVE-2025-4945,CVE-2025-6052,CVE-2025-3512,CVE-2024-56431,CVE-2025-24031,CVE-2025-24511,CVE-2025-2588,CVE-2025-6199,CVE-2025-32415,CVE-2025-43965,CVE-2025-48708,CVE-2025-30258,CVE-2023-47466,CVE-2025-6170)
Description	Oracle has released monthly security updates addressing multiple vulnerabilities that exist in their product. These vulnerabilities could be exploited by malicious users to compromise the affected system. Oracle advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Oracle Solaris 11.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.oracle.com/security-alerts/bulletinjul2025.html

Affected Product	**IBM**
Severity	**Low**
Affected Vulnerability	Security Restrictions Bypass Vulnerability (CVE-2024-56339)
Description	IBM has released a security update addressing a security restrictions bypass vulnerability that exists in their products. **CVE-2024-56339** - IBM WebSphere Application Server and IBM WebSphere Application Server Liberty could allow a remote attacker to bypass security restrictions caused by a failure to honor security configuration. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM WebSphere Application Server Versions - 9.0 IBM WebSphere Application Server Liberty Versions - 17.0.0.3 - 25.0.0.7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7239955

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.