Advisory Alert

Alert Number: AAA20260529 **Date:** May 29, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
Veeam	**Critical**	Remote Code Execution Vulnerability
Drupal	**Critical**	PHP Code Execution Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
Samba	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
Veeam	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
Asus	**High**	Security Update
Samba	**High, Medium**	Multiple Vulnerabilities
Oracle	**High, Medium**	Multiple Vulnerabilities
IBM	**High, Medium, Low**	Multiple Vulnerabilities

Description

Vendor	**Veeam**
Severity	**Critical**
Affected Vulnerability	Remote Code Execution Vulnerability (CVE-2026-32998)
Description	Veeam has released a security update addressing a vulnerability that exists in their product. **CVE-2026-32998**: A critical vulnerability in in Veeam Service Provider Console, affecting version 9.2.0.33215 and all earlier version 9 builds. Successful exploitation could allow an attacker to execute arbitrary code remotely on affected systems. Veeam advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Veeam Service Provider Console 9.2.0.33215 and all earlier version 9 builds
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.veeam.com/kb4853

Vendor	**Drupal**
Severity	**Critical**
Affected Vulnerability	PHP Code Execution Vulnerability (CVE-2026-9726)
Description	Drupal has released a security update addressing a vulnerability that exists in their product. **CVE-2026-9726:** The Basket module does not sufficiently sanitize user-supplied data before passing it to PHP's unserialize().An attacker can supply a crafted payload and trigger PHP Object Injection. If a viable gadget chain exists in the site codebase or installed dependencies, this can result in arbitrary PHP code execution. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Drupal AlternativeCommerce (Basket Module) – Versions prior to 2.1.17
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2026-038

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-8633, CVE-2025-3357, CVE-2025-30065, CVE-2026-33228, CVE-2026-4800, CVE-2026-27837, CVE-2026-0848, CVE-2026-25547, CVE-2026-27699, CVE-2026-1525, CVE-2026-25896, CVE-2025-14009, CVE-2026-27459, CVE-2026-33937, CVE-2025-62718, CVE-2026-29063)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their product. These vulnerabilities could be exploited by malicious users to compromise affected systems. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Cloud Pak System Versions (Power): • 2.3.3.7 & 2.3.3.7 IFix 1 • 2.3.5.0 IBM Cloud Pak System Versions (Intel): • 2.3.3.6, 2.3.3.6 iFix1 & 2.3.3.6 iFix2 • 2.3.4.0, 2.3.4.1 & 2.3.4.1 iFix1 IBM Cloud Pak for Security – Versions - 1.10.0.0 - 1.10.11.0 QRadar Suite Software – Versions 1.10.12.0 - 1.11.10.0 IBM Security SOAR Versions: • 51.0.9.0 to 51.0.9.2 • 51.0.8.0 to 51.0.8.2 • 51.0.7.0 to 51.0.7.2 • 51.0.6.0 to 51.0.6.2 IBM Web Server Plug-ins for IBM WebSphere Application Server and IBM WebSphere Liberty – Versions 8.5, 9.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7274072 • https://www.ibm.com/support/pages/node/7240254 • https://www.ibm.com/support/pages/node/7274154 • https://www.ibm.com/support/pages/node/7274313 • https://www.ibm.com/support/pages/node/7274315

Vendor	**Samba**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-4408, CVE-2026-4480)
Description	Samba has released a security update addressing multiple vulnerabilities that exist in their product. **CVE-2026-4408:** Samba file servers and classic (non-AD) domain controllers with samba-dcerpcd started as a system service and with a "check password script" that has the %u substitution character are vulnerable to a remote code execution. **CVE-2026-4480:** Samba print servers with a "print command" that has the %J substitution character are vulnerable to a Remote Code Execution. Samba advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Samba DCE/RPC SAMR server – All versions Samba printing subsystem – All versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.samba.org/samba/history/security.html

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-21999, CVE-2025-38653, CVE-2025-39766, CVE-2025-39981, CVE-2025-68183, CVE-2025-68347, CVE-2025-68366, CVE-2025-68741, CVE-2025-71116, CVE-2026-23243, CVE-2026-23270, CVE-2026-23455, CVE-2026-31408, CVE-2026-31419, CVE-2026-31532, CVE-2026-31684, CVE-2026-31685, CVE-2026-31709, CVE-2026-43020, CVE-2026-43027, CVE-2026-43051, CVE-2026-43158, CVE-2026-43163, CVE-2026-43190)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in the kernel of their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux for IBM z Systems 8 s390x Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for ARM 64 8 aarch64 Red Hat CodeReady Linux Builder for x86_64 8 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le Red Hat CodeReady Linux Builder for ARM 64 8 aarch64 Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 8.10 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 8.10 aarch64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 8.10 ppc64le Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 8.10 s390x Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64 Red Hat Enterprise Linux Server - AUS 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 - Extended Life Cycle 9.4 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 9.4 aarch64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.4 ppc64le Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 9.4 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:21706 • https://access.redhat.com/errata/RHSA-2026:21209

Vendor	**Veeam**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-32996, CVE-2026-32997)
Description	Veeam has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-32996:** A vulnerability in Veeam Agent for Microsoft Windows. Successful exploitation could allow a local attacker to escalate their privileges on the affected system. **CVE-2026-32997:** A vulnerability allowing an authenticated user with the Backup Administrator role to write arbitrary files on a Linux-based Veeam Backup & Replication server (Veeam Software Appliance). Veeam advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Veeam Backup & Replication 13.0.1.2067 and all earlier version 13 builds.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.veeam.com/kb4852

Vendor	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released a security update addressing multiple vulnerabilities that exist in the third party components of their product. These vulnerabilities could be exploited by malicious users to compromise affected systems. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell Enterprise SONiC Distribution – Versions prior to 4.5.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000470137/dsa-2026-241-security-update-for-dell-enterprise-sonic-distribution-vulnerabilities

Vendor	**Asus**
Severity	**High**
Affected Vulnerability	Security Update (CVE-2026-7480)
Description	Asus has released a security update addressing a vulnerability that exists in their product. **CVE-2026-7480:** An Incorrect Permission Assignment for Critical Resource vulnerability in ASUS System Control Interface allows a local user to elevate privileges to SYSTEM and execute arbitrary code via a crafted RPC call that bypass the validation mechanism. Asus advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	ASUS System Control Interface Versions: • 3.1.59.0 (x64) and earlier • 3.2.60.0 (ARM) and earlier
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.asus.com/security-advisory

Vendor	**Samba**
Severity	**High, Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-2340, CVE-2026-3012, CVE-2026-3238, CVE-2026-1933)
Description	Samba has released a security update addressing multiple vulnerabilities that exists in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Samba advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	All versions since Samba 4.21
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.samba.org/samba/history/security.html

Vendor	**Oracle**
Severity	**High,** Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-46833, CVE-2026-46834, CVE-2026-46835, CVE-2026-46840, CVE-2026-46775, CVE-2026-46839, CVE-2026-2332, CVE-2026-35277, CVE-2026-35266, CVE-2026-46829, CVE-2026-46842, CVE-2026-46843, CVE-2026-46841, CVE-2026-46830, CVE-2026-5795, CVE-2026-4800, CVE-2025-13465, CVE-2026-2950, CVE-2026-33557, CVE-2025-15467, CVE-2026-41044, CVE-2025-58050, CVE-2026-34487, CVE-2026-24308, CVE-2026-25646, CVE-2026-34059, CVE-2026-40466, CVE-2026-41043, CVE-2025-14017, CVE-2026-21998, CVE-2026-22001, CVE-2026-22002, CVE-2026-22004, CVE-2026-22005, CVE-2026-22009, CVE-2026-22015, CVE-2026-22017, CVE-2026-34270, CVE-2026-34271, CVE-2026-34276, CVE-2026-34303, CVE-2026-34304, CVE-2026-34308, CVE-2026-35236, CVE-2026-35237, CVE-2026-35238, CVE-2026-35239, CVE-2026-35240, CVE-2026-35554, CVE-2026-23918, CVE-2026-24072, CVE-2026-28780, CVE-2026-29168, CVE-2026-29169, CVE-2026-33006, CVE-2026-33007, CVE-2026-33523, CVE-2026-33857, CVE-2026-34032, CVE-2026-24281, CVE-2026-29145, CVE-2026-34483, CVE-2026-34486, CVE-2026-34500, CVE-2026-46822, CVE-2026-46824, CVE-2026-46817, CVE-2026-46819, CVE-2026-46837, CVE-2026-46827, CVE-2026-46826, CVE-2026-46820, CVE-2026-46828, CVE-2026-46821, CVE-2026-46823, CVE-2026-46818, CVE-2026-34311)
Description	Oracle has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Oracle advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Oracle Communications Unified Assurance – Versions 6.1.1 - 7.0.0 Oracle Database Server – Versions 23.4.0-23.26.2 Oracle E-Business Suite – Versions 12.2.3-12.2.15 Oracle Hospitality OPERA 5 Property Services – Versions 5.6.19.24, 5.6.22, 5.6.25.19, 5.6.27.6, 5.6.28 Oracle REST Data Services – Versions 24.2.0-26.1.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.oracle.com/security-alerts/cspumay2026.html

Vendor	**IBM**
Severity	**High,** Medium, Low
Affected Vulnerability	Multiple Vulnerabilities
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Cloud Pak System Versions (Power): • 2.3.3.7 & 2.3.3.7 IFix 1 • 2.3.5.0 IBM Cloud Pak System Versions (Intel): • 2.3.3.6, 2.3.3.6 iFix1 & 2.3.3.6 iFix2 • 2.3.4.0, 2.3.4.1 & 2.3.4.1 iFix1 IBM Db2 Versions: • 11.5.0 - 11.5.9 • 12.1.0 - 12.1.4 Platform Navigator in IBM Cloud Pak for Integration (CP4I) • 16.1.0 to 16.1.0.22 • 16.1.1 & 16.1.2 • 16.1.3.0 to 16.1.3.4 Automation Assets in IBM Cloud Pak for Integration (CP4I) • 4.0.0-sc2 to 4.0.19-sc2 • 4.1.0 & 4.2.0 • 4.3.0 to 4.3.3 IBM Cloud Pak for Security – Versions - 1.10.0.0 - 1.10.11.0 QRadar Suite Software – Versions 1.10.12.0 - 1.11.10.0 IBM Security SOAR Versions: • 51.0.9.0 to 51.0.9.2 • 51.0.8.0 to 51.0.8.2 • 51.0.7.0 to 51.0.7.2 • 51.0.6.0 to 51.0.6.2 IBM WebSphere Remote Server – Versions 8.5, 9.0, 9.1 IBM Web Server Plug-ins for IBM WebSphere Application Server and IBM WebSphere Liberty – Versions 8.5, 9.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7274072 • https://www.ibm.com/support/pages/node/7240254 • https://www.ibm.com/support/pages/node/7274154 • https://www.ibm.com/support/pages/node/7274313 • https://www.ibm.com/support/pages/node/7274315 • https://www.ibm.com/support/pages/node/7274366 • https://www.ibm.com/support/pages/node/7274369 • https://www.ibm.com/support/pages/node/7274368 • https://www.ibm.com/support/pages/node/7274303 • https://www.ibm.com/support/pages/node/7274300 • https://www.ibm.com/support/pages/node/7274312 • https://www.ibm.com/support/pages/node/7273554

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.