TLP: WHITE

Advisory Alert

Alert Number: AAA20260225 **Date:** February 25, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SolarWinds	**Critical**	Remote Code Execution Vulnerabilities
IBM	**Critical**	Buffer Overflow Vulnerability
SUSE	**High**	Multiple Vulnerabilities
Broadcom VMware	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
AMD	**High**	Denial of Service Vulnerability
Lenovo	**High**	Denial of Service Vulnerability
Red Hat	**High**, Medium	Multiple Vulnerabilities
Ubuntu	**High**, Medium	Multiple Vulnerabilities
IBM	**High**, Medium, Low	Multiple Vulnerabilities
HPE	Medium	Denial of Service Vulnerability
SonicWall	Medium	Multiple Vulnerabilities
F5	Medium	Integer Overflow Vulnerability

Description

Affected Product	**SolarWinds**
Severity	**Critical**
Affected Vulnerability	Remote Code Execution Vulnerabilities (CVE-2025-40541, CVE-2025-40538, CVE-2025-40539, CVE-2025-40540)
Description	SolarWinds has released security updates addressing multiple vulnerabilities that exist in their Serv-U product. These vulnerabilities could be exploited by malicious users to conduct remote code execution attacks. SolarWinds advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	SolarWinds Serv-U 15.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.solarwinds.com/trust-center/security-advisories/cve-2025-40541 • https://www.solarwinds.com/trust-center/security-advisories/cve-2025-40538 • https://www.solarwinds.com/trust-center/security-advisories/cve-2025-40539 • https://www.solarwinds.com/trust-center/security-advisories/cve-2025-40540

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Buffer Overflow Vulnerability (CVE-2026-1188)
Description	IBM has released security updates addressing a vulnerability that exists in their WebSphere products. **CVE-2026-1188**: In the Eclipse OMR port library component since release 0.2.0, an API function to return the textual names of all supported processor features was not accounting for the separator inserted between processor features. If the output buffer supplied to this function was incorrectly sized, failing to account for the separator when determining when a write to the buffer was safe could lead to a buffer overflow. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	WebSphere Service Registry and Repository Studio versions 8.5 to 8.5.6.3 WebSphere Service Registry and Repository versions 8.5 to 8.5.6.3 IBM WebSphere Application Server versions 9.0 IBM WebSphere Application Server versions 8.5.0.0 to 8.5.5.28 IBM WebSphere Application Server – Liberty Continuous delivery version
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7259945 • https://www.ibm.com/support/pages/node/7259445

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released a security update addressing multiple vulnerabilities that exists in the Linux kernel utilized by their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. SUSE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	openSUSE Leap 15.4 SUSE Linux Enterprise High Availability Extension 15 SP4 SUSE Linux Enterprise High Performance Computing 15 SP4 SUSE Linux Enterprise High Performance Computing ESPOS 15 SP4 SUSE Linux Enterprise High Performance Computing LTSS 15 SP4 SUSE Linux Enterprise Live Patching 15-SP4 SUSE Linux Enterprise Micro 5.3 SUSE Linux Enterprise Micro 5.4 SUSE Linux Enterprise Micro for Rancher 5.3 SUSE Linux Enterprise Micro for Rancher 5.4 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Server 15 SP4 SUSE Linux Enterprise Server 15 SP4 LTSS SUSE Linux Enterprise Server for SAP Applications 15 SP4 SUSE Manager Proxy 4.3 SUSE Manager Retail Branch Server 4.3 SUSE Manager Server 4.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20260617-1/

Affected Product	**Broadcom VMware**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-22719, CVE-2026-22720, CVE-2026-22721)
Description	Broadcom has released a security update addressing multiple vulnerabilities that exists in their products. **CVE-2026-22719**: A malicious unauthenticated actor may exploit this issue to execute arbitrary commands which may lead to remote code execution in VMware Aria Operations while support-assisted product migration is in progress **CVE-2026-22720**: A malicious actor with privileges to create custom benchmarks may be able to inject script to perform administrative actions in VMware Aria Operations. **CVE-2026-22721**: A malicious actor with privileges in vCenter to access Aria Operations may leverage this vulnerability to obtain administrative access in VMware Aria Operations. Broadcom advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	• VMware Cloud Foundation 9.x.x.x versions prior to 9.0.2.0 • VMware vSphere Foundation 9.x.x.x versions prior to 9.0.2.0 • VMware Aria Operations 8.x versions prior to 8.16.6 • VMware Cloud Foundation (Aria Operations Component) 5.x, 4.x versions prior to KB92148 • VMware Telco Cloud Platform (Aria Operations Component) 5.x, 4.x versions prior to KB428241 • VMware Telco Cloud Infrastructure (Aria Operations Component) 3.x, 2.x versions prior to KB428241
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/security-advisories/0/36947

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-52615, CVE-2025-40780, CVE-2025-40778, CVE-2024-25621, CVE-2025-64329, CVE-2025-11563, CVE-2025-1352, CVE-2025-1372, CVE-2025-1376, CVE-2025-1377, CVE-2025-30258, CVE-2022-50116, CVE-2024-53177, CVE-2024-58239, CVE-2025-38180, CVE-2025-38323, CVE-2025-38352, CVE-2025-38460, CVE-2025-38498, CVE-2025-38499, CVE-2025-38546, CVE-2025-38555, CVE-2025-38560, CVE-2025-38563, CVE-2025-38608, CVE-2025-38617, CVE-2025-38618, CVE-2025-38644, CVE-2025-9086, CVE-2025-10148, CVE-2025-11731, CVE-2025-10911, CVE-2025-9187, CVE-2025-53066, CVE-2025-53057, CVE-2025-9230, CVE-2025-41244, CVE-2025-6069, CVE-2025-8194, CVE-2025-52565, CVE-2025-31133, CVE-2025-52881, CVE-2025-58143, CVE-2025-27466, CVE-2025-58142, CVE-2025-58147, CVE-2025-58148, CVE-2026-22765, CVE-2026-22766, CVE-2026-23858, CVE-2026-23859)
Description	Dell has released security updates addressing multiple vulnerabilities that exists in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	PowerStore 500T PowerStoreT OS Versions prior to 4.3.1.0-2662695 PowerStore 1000T PowerStoreT OS Versions prior to 4.3.1.0-2662695 PowerStore 1200T PowerStoreT OS Versions prior to 4.3.1.0-2662695 PowerStore 3000T PowerStoreT OS Versions prior to 4.3.1.0-2662695 PowerStore 3200Q PowerStoreT OS Versions prior to 4.3.1.0-2662695 PowerStore 3200T PowerStoreT OS Versions prior to 4.3.1.0-2662695 PowerStore 5000T PowerStoreT OS Versions prior to 4.3.1.0-2662695 PowerStore 5200Q PowerStoreT OS Versions prior to 4.3.1.0-2662695 PowerStore 5200T PowerStoreT OS Versions prior to 4.3.1.0-2662695 PowerStore 7000T PowerStoreT OS Versions prior to 4.3.1.0-2662695 PowerStore 9000T PowerStoreT OS Versions prior to 4.3.1.0-2662695 PowerStore 9200T PowerStoreT OS Versions prior to 4.3.1.0-2662695 Dell Wyse Management Suite Versions prior to 5.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000432173/dsa-2026-115-dell-powerstore-t-security-update-for-multiple-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000429141/dsa-2026-103

Affected Product	**AMD**
Severity	**High**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2023-31364)
Description	AMD has released a security update addressing a vulnerability that exists in their products. **CVE-2023-31364**: Improper handling of direct memory writes in the input-output memory management unit could allow a malicious guest virtual machine (VM) to flood a host with writes, potentially causing a fatal machine check error resulting in denial of service. AMD advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	AMD EPYC™ 7001 Series Processors versions prior to NaplesPI 1.0.0.R AMD EPYC™ 7002 Series Processors versions prior to RomePI 1.0.0.N AMD EPYC™ 7003 Series Processors versions prior to MilanPI 1.0.0.H AMD EPYC™ 8004 Series Processors versions prior to GenoaPI 1.0.0.G AMD EPYC™ 9004 Series Processors versions prior to GenoaPI 1.0.0.G AMD EPYC™ 9005 Series Processors versions prior to TurinPI 1.0.0.7 AMD EPYC™ Embedded 3000 Series Processors versions prior to SnowyOwl_SP4_SP4r2.1.1.0.H AMD EPYC™ Embedded 7002 Series Processors versions prior to EmbRomePI-SP3 1.0.0.F AMD EPYC™ Embedded 7003 Series Processors versions prior to EmbMilanPI-SP3 v9 1.0.0.C AMD EPYC™ Embedded 8004 Series Processors versions prior to EmbGenoaPI-SP5 1.0.0.B AMD EPYC™ Embedded 9004 Series Processors versions prior to EmbGenoaPI-SP5 1.0.0.B AMD EPYC™ Embedded 9005 Series Processors versions prior to EmbTurinPI-SP5 1.0.0.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-7059.html

Affected Product	**Lenovo**
Severity	**High**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2023-31364)
Description	Lenovo has released a security update addressing a vulnerability that exists in their products. **CVE-2023-31364**: Improper handling of direct memory writes in the input-output memory management unit could allow a malicious guest virtual machine (VM) to flood a host with writes, potentially causing a fatal machine check error resulting in denial of service. Lenovo advises to apply these security fixes at your earliest to protect your systems from potential threats.

Affected Products	• Lenovo System UEFI/BIOS Firmware versions prior to KAE142F-5.80 for
	  ○ HX645 V3 Integrated System (ThinkAgile)
	  ○ HX665 V3 Certified Node (ThinkAgile)
	  ○ HX645 V3 Certified Node (ThinkAgile)
	  ○ HX665 V3 Integrated System (ThinkAgile)
	  ○ HX665 V3 Storage Certified Node (ThinkAgile)
	  ○ VX635 V3 Certified Node (ThinkAgile)
	  ○ VX635 V3 Integrated System (ThinkAgile)
	  ○ VX645 V3 Certified Node (ThinkAgile)
	  ○ VX645 V3 Integrated System (ThinkAgile)
	  ○ VX655 V3 Certified Node (ThinkAgile)
	  ○ VX655 V3 Integrated System (ThinkAgile)
	  ○ VX665 V3 Certified Node (ThinkAgile)
	  ○ VX665 V3 Integrated System (ThinkAgile)
	• SE455 V3 / SE455i V3 (ThinkEdge) Lenovo System UEFI/BIOS Firmware versions prior to MBE122F-6.40
	• SD535 V3 (ThinkSystem) Lenovo System UEFI/BIOS Firmware versions prior to GPE124F-5.40
	• SD665 V3 (ThinkSystem) Lenovo System UEFI/BIOS Firmware versions prior to QGE144D-8.40
	• SR635 V3 (ThinkSystem) Lenovo System UEFI/BIOS Firmware versions prior to KAE142F-5.80
	• SR645 V3 (ThinkSystem) Lenovo System UEFI/BIOS Firmware versions prior to KAE142F-5.80
	• SR655 V3 (ThinkSystem) Lenovo System UEFI/BIOS Firmware versions prior to KAE142F-5.80
	• SR665 V3 (ThinkSystem) Lenovo System UEFI/BIOS Firmware versions prior to KAE142F-5.80
	• SR675 V3 / SR675i V3 (ThinkSystem) Lenovo System UEFI/BIOS Firmware versions prior to QGE144D-8.40
	• SR685a V3 (ThinkSystem) Lenovo System UEFI/BIOS Firmware versions prior to R5E120E-4.30

Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.lenovo.com/us/en/product_security/LEN-212127

Affected Product	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-38206, CVE-2025-40096, CVE-2025-40168, CVE-2025-68800, CVE-2025-38022, CVE-2025-38415, CVE-2025-38459, CVE-2025-39760, CVE-2025-39933, CVE-2025-40271, CVE-2023-53821, CVE-2026-23074, CVE-2025-37882, CVE-2025-37861, CVE-2023-53192, CVE-2023-53762, CVE-2025-40269, CVE-2022-50673, CVE-2025-68349)
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 systems. Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Red Hat CodeReady Linux Builder for ARM 64 10 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems 10 s390x Red Hat CodeReady Linux Builder for Power, little endian 10 ppc64le Red Hat CodeReady Linux Builder for x86_64 10 x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.2 aarch64 Red Hat Enterprise Linux for ARM 64 10 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.2 s390x Red Hat Enterprise Linux for IBM z Systems 10 s390x Red Hat Enterprise Linux for Power, little endian 10 ppc64le Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.6 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64 Red Hat Enterprise Linux for x86_64 10 x86_64 Red Hat Enterprise Linux Server - AUS 8.6 x86_64 Red Hat Enterprise Linux Server - AUS 9.2 x86_64 Red Hat Enterprise Linux Server - TUS 8.6 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:3275 • https://access.redhat.com/errata/RHSA-2026:3268 • https://access.redhat.com/errata/RHSA-2026:3267

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-53217, CVE-2024-50299, CVE-2025-21780, CVE-2022-49267, CVE-2025-37899, CVE-2025-22037)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in the Linux kernel utilized by their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Ubuntu advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Ubuntu versions 14.04, 20.04, 22.04 and 24.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-8061-1 • https://ubuntu.com/security/notices/USN-8060-1 • https://ubuntu.com/security/notices/USN-8059-1

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-36009, CVE-2025-62230, CVE-2025-62231, CVE-2025-8732)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected products. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Db2 Server versions 11.5.0 to 11.5.9 and 12.1.0 to 12.1.3 AIX versions 7.2 AIX versions 7.3 VIOS versions 4.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7257623 • https://www.ibm.com/support/pages/node/7261396 • https://www.ibm.com/support/pages/node/7261170

Affected Product	**HPE**
Severity	**Medium**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2023-31364)
Description	HPE has released security updates addressing a vulnerability that exists in their products. **CVE-2023-31364**: Improper handling of direct memory writes in the input-output memory management unit could allow a malicious guest virtual machine (VM) to flood a host with writes, potentially causing a fatal machine check error resulting in denial of service. HPE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	HPE SimpliVity 325 Gen11 - Prior to SimpliVity Support Pack (SVTSP) Gen11 v2026_0116 HPE ProLiant Compute DL325 Gen12 - Prior to v1.34_11-28-2025 HPE ProLiant Compute DL345 Gen12 - Prior to v1.34_11-28-2025 HPE ProLiant DL145 Gen11 - Prior to v1.70_08-07-2025 HPE ProLiant DL325 Gen11 Server - Prior to v2.70_08-07-2025 HPE ProLiant DL345 Gen11 Server - Prior to v2.70_08-07-2025 HPE ProLiant DL365 Gen11 Server - Prior to v2.70_08-07-2025 HPE ProLiant DL385 Gen11 Server - Prior to v2.70_08-07-2025 HPE ProLiant DL325 Gen10 Plus v2 server - Prior to v3.90_10-03-2025 HPE ProLiant DL325 Gen10 Plus server - Prior to v3.90_10-03-2025 HPE ProLiant DL345 Gen10 Plus server - Prior to v3.90_10-03-2025 HPE ProLiant DL365 Gen10 Plus server - Prior to v3.90_10-03-2025 HPE ProLiant DL385 Gen10 Plus server - Prior to v3.90_10-03-2025 HPE ProLiant DL385 Gen10 Plus v2 server - Prior to v3.90_10-03-2025 HPE ProLiant XL225n Gen10 Plus 1U Node - Prior to v3.90_10-03-2025 HPE ProLiant DL325 Gen10 Server - Prior to v3.80_09-05-2025 HPE ProLiant DL385 Gen10 Server - Prior to v3.80_09-05-2025
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05023en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05021en_us&docLocale=en_US

Affected Product	**SonicWall**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-0399, CVE-2026-0400, CVE-2026-0401, CVE-2026-0402)
Description	SonicWall has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to conduct Buffer Overflow, and Out-of-bounds Read attacks. SonicWall advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Versions 7.0.1-5169 and older / 7.3.1-7013 and older • Gen7 hardware Firewalls - TZ270, TZ270W, TZ370, TZ370W, TZ470, TZ470W, TZ570, TZ570W, • TZ570P, TZ670, NSa 2700, NSa 3700,NSa 4700, NSa 5700, NSa 6700, NSsp 10700, NSsp 11700, NSsp 13700, NSsp 15700 • Gen7 virtual Firewalls (NSv) - NSV270, NSv470, NSv870 (ESX, KVM, HYPER-V, AWS, Azure) Versions 8.1.0-8017 and older • Gen8 Firewalls - TZ80, TZ280, TZ380, TZ480, TZ580, TZ680, NSa 2800, NSa 3800, NSa 4800, NSa 5800
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0001

Affected Product	**F5**
Severity	**Medium**
Affected Vulnerability	Integer Overflow Vulnerability (CVE-2025-47268)
Description	F5 has released a security update addressing a vulnerability that exists in the iputils component which is utilized by their products. **CVE-2025-47268**: A malicious, authenticated user with administrator privileges and Advanced Shell (bash) access may be able to exploit this vulnerability by causing the ping utility to terminate or report incorrect Round Trip Time (RTT) statistics. F5 advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	BIG-IP (all modules) • versions 17.5.0 to 17.5.1 • versions 17.1.0 to 17.1.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000158112

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.