Advisory Alert

Alert Number: AAA20260511 **Date:** May 11, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Code Injection Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
Barracuda	**High**	Local Privilege Escalation Vulnerability
SUSE	**High**	Multiple Vulnerabilities
cPanel	**High**, **Medium**, **Low**	Multiple Vulnerabilities
IBM	**Medium**	Prototype Pollution Vulnerability

Description

Affected Product	**Dell**
Severity	**Critical**
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 affected systems. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Elastic Cloud Storage (ECS) - Versions 3.8.1.0 through 3.8.1.7 ObjectScale - Versions prior to 4.3.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000462117/dsa-2026-047-security-update-for-dell-ecs-and-objectscale-multiple-vulnerabilities-1

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Code Injection Vulnerability (CVE-2026-4800)
Description	IBM has released a security update addressing a vulnerability that exists in their products. **CVE-2026-4800** - When an application passes untrusted input as options.imports key names, an attacker can inject default-parameter expressions that execute arbitrary code at template compilation time. Additionally, _.template uses assignInWith to merge imports, which enumerates inherited properties via for..in. If Object.prototype has been polluted by any other vector, the polluted keys are copied into the imports object and passed to Function(). IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Platform Navigator: • 16.1.0 – 16.1.0.22 • 16.1.1, 16.1.2 • 16.1.3.0 – 16.1.3.5 Automation Assets: • 4.0.0-sc2 – 4.0.19-sc2 • 4.1.0, 4.2.0, 4.3.0 • 4.3.0 – 4.3.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7272406

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-23097, CVE-2026-23139, CVE-2026-23243, CVE-2026-23401, CVE-2026-31402, CVE-2026-31532)
Description	Red Hat has released a security update addressing multiple vulnerabilities that exist in the kernel component 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 - Extended Update Support 10.0 x86_64 • Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 10.0 s390x • Red Hat Enterprise Linux for Power, little endian - Extended Update Support 10.0 ppc64le • Red Hat Enterprise Linux for ARM 64 - Extended Update Support 10.0 aarch64 • Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 10.0 x86_64 • Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 10.0 ppc64le • Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 10.0 s390x • Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 10.0 aarch64 • Red Hat Enterprise Linux for ARM 64 - 4 years of updates 10.0 aarch64 • Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 10.0 s390x • Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.0 ppc64le • Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.0 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:15883

Affected Product	**Barracuda**
Severity	**High**
Affected Vulnerability	Local Privilege Escalation Vulnerability (CVE-2026-31431)
Description	Barracuda has released a security update addressing a vulnerability that exist in a kernel module of their products. **CVE-2026-31431** - This vulnerability exploits a flaw in how the kernel handles splice() operations targeting AF_ALG (Authenticated Encryption with Associated Data) sockets. Barracuda advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Barracuda CloudGen Firewall Barracuda SecureEdge
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://trust.barracuda.com/security/information/linux-kernel-local-privilege-escalation-lpe

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released a security update addressing a vulnerability that exist in the kernel of their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.4, 15.5, and 15.6 SUSE Linux Enterprise Micro 5.3, 5.4, and 5.5 SUSE Linux Enterprise Server 11 SP4 (including LTSS Extreme Core) SUSE Linux Enterprise 12 SP5 (Server, SAP, Live Patching, and High Performance Computing) SUSE Linux Enterprise 15 SP4 (Server, SAP, Live Patching, Real Time, and High Performance Computing) SUSE Linux Enterprise 15 SP5 (Server, SAP, Live Patching, Real Time, and High Performance Computing) SUSE Linux Enterprise 15 SP6 (Server, SAP, Live Patching, and Real Time) SUSE Linux Enterprise 15 SP7 (Server, SAP, Live Patching, Real Time, and Real Time Module)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2026/suse-su-20261765-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20261767-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20261768-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20261770-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20261771-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20261775-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20261776-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20261777-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20261778-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20261773-1/

Affected Product	**cPanel**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-29201, CVE-2026-29202, CVE-2026-29203, CVE-2026-6735, CVE-2026-7259, CVE-2025-14179, CVE-2026-6722, CVE-2026-7261, CVE-2026-7262, CVE-2026-7568, CVE-2026-7258)
Description	cPanel 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. cPanel advises to apply security fixes at your earliest to protect systems from potential threats.

Affected Products	• cPanel & WHM versions prior to 136.0.9
	• EasyApache 25.58
	  ○ ea-php82 versions prior to 8.2.31
	  ○ ea-php83 versions prior to 8.3.31
	  ○ ea-php84 versions prior to 8.4.21
	  ○ ea-php85 versions prior to 8.5.6

Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://docs.cpanel.net/changelogs/136-change-log/#13609 https://docs.cpanel.net/changelogs/easyapache-4-change-log-25/#2558

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Prototype Pollution Vulnerability (CVE-2026-2950)
Description	IBM has released a security update addressing a vulnerability that exists in their products. **CVE-2026-2950** - Lodash versions 4.17.23 and earlier are vulnerable to prototype pollution in the _.unset and _.omit functions. An attacker can bypass the check by passing array-wrapped path segments. This allows deletion of properties from built-in prototypes such as Object.prototype, Number.prototype, and String.prototype. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Platform Navigator: • 16.1.0 – 16.1.0.22 • 16.1.1, 16.1.2 • 16.1.3.0 – 16.1.3.5 Automation Assets: • 4.0.0-sc2 – 4.0.19-sc2 • 4.1.0, 4.2.0, 4.3.0 • 4.3.0 – 4.3.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7272406

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.