Advisory Alert

Alert Number: AAA20260914 **Date:** September 14, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
MongoDB	**High**	Race Condition Vulnerability
NetApp	**High**	Security Update
WatchGuard	**Medium**	Information Disclosure Vulnerability
IBM	**Medium**, **Low**	Multiple Vulnerabilities

Description

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-52933, CVE-2026-53196, CVE-2026-64387)
Description	Red Hat has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-52933:** A flaw was found in the Linux kernel's io_uring/poll component. A logic error exists in the io_poll_get_ownership() function due to an incorrect signed comparison. This flaw prevents the necessary slowpath from being triggered when the IO_POLL_CANCEL_FLAG is set, potentially leading to unexpected behavior or resource mismanagement within the kernel. **CVE-2026-53196:** A flaw was found in the Linux kernel's io_ti USB serial driver. A malicious USB device, when plugged into a host running this driver, can exploit a heap overflow vulnerability in the get_manuf_info() function. This occurs because the driver does not properly validate the size of data read from the device's I2C EEPROM against the allocated memory buffer. This improper validation can lead to out-of-bounds memory writes, potentially allowing an attacker to execute arbitrary code or cause a system crash (Denial of Service). **CVE-2026-64387:** A flaw was found in the Linux kernel's Server Message Block (SMB) client. This vulnerability, a double-free error, occurs when the client attempts to free the same memory buffer twice during a directory query operation. An attacker could potentially exploit this flaw to cause memory corruption, leading to a denial of service or, in some cases, arbitrary code execution. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux (RHEL) 10.0: • CodeReady Linux Builder (Extended Update Support 10.0): aarch64, ppc64le, s390x, x86_64 • Red Hat Enterprise Linux (4 Years of Updates / Support 10.0): aarch64, ppc64le, s390x, x86_64 • Red Hat Enterprise Linux (Extended Update Support 10.0): aarch64, ppc64le, s390x, x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:67114

Vendor	**MongoDB**
Severity	**High**
Affected Vulnerability	Race Condition Vulnerability (CVE-2026-89099)
Description	MongoDB has released a security update addressing a vulnerability that exist in their products. **CVE-2026-89099:** A race condition in the document value layer of MongoDB Server can allow concurrent server threads to operate on the same internal memory without synchronization, leading to memory corruption. An authenticated user holding ordinary read-write privileges on a database may be able to trigger this condition over the normal client protocol, resulting in server termination and potential corruption of process memory with user-influenced content. MongoDB advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	MongoDB Server: • 7.0 Series: Prior to 7.0.43 • 8.0 Series: Prior to 8.0.32 • 8.3 Series: Prior to 8.3.11
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.mongodb.com/resources/products/alerts#security

Vendor	**NetApp**
Severity	**High**
Affected Vulnerability	Security Update (CVE-2026-23066)
Description	NetApp has released a security update addressing a vulnerability that exist in their products. **CVE-2026-23066**: Linux kernel versions 4.11 prior to 6.18.8 and 6.19-rc1 through 6.19-c6 are susceptible to a vulnerability which when successfully exploited could lead to disclosure of sensitive information, addition or modification of data, or Denial of Service (DoS). NetApp advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	ONTAP tools for VMware vSphere 10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20260911-0019

Vendor	**WatchGuard**
Severity	**Medium**
Affected Vulnerability	Information Disclosure Vulnerability (CVE-2003-0001)
Description	WatchGuard has released a security update addressing a vulnerability that exist in their products. **CVE-2003-0001:** Multiple ethernet Network Interface Card (NIC) device drivers do not pad frames with null bytes, which allows remote attackers to obtain information from previous packets or kernel memory by using malformed packets, as demonstrated by Etherleak. WatchGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	WatchGuard Fireware OS: • 12.0.0 – 12.12.0 (Prior to 12.12.1) • 2025.0 – 2026.2.0 (Prior to 2026.2.1)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.watchguard.com/WGSA-2026-0031/

Vendor	**IBM**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-73281, CVE-2026-73283, CVE-2026-73282)
Description	IBM has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-73281:** In ssh-agent in OpenSSH before 10.5, some operations can occur remotely but were intended to occur only locally, including operations that add tokens or use keys. This is caused by misinteraction between agent locking and the session-bind@openssh.com extension. **CVE-2026-73282:** In ssh in OpenSSH before 10.5, a use-after-free for realloc data can occur if a certain pair of remote-forwarding operations are concurrent. **CVE-2026-73283:** In sshd in OpenSSH before 10.5, the restrict keyword (in authorized_keys) was supposed to be applicable to tunnel forwarding but was not. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Power Systems & Operating Systems: • IBM AIX: 7.2, 7.3 • IBM PowerVM Virtual I/O Server (VIOS): 4.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7287147

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.