TLP: WHITE

Advisory Alert

Alert Number: AAA20260526 **Date:** May 26, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Zyxel Networks	**Medium**	Missing Authorization Vulnerability

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2006-10003, CVE-2026-31402, CVE-2026-6100)
Description	IBM has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2006-10003**: XML::Parser versions through 2.47 for Perl has an off-by-one heap buffer overflow in st_serial_stack. In the case (stackptr == stacksize - 1), the stack will NOT be expanded. Then the new value will be written at location (++stackptr), which equals stacksize and therefore falls just outside the allocated buffer. The bug can be observed when parsing an XML file with very deep element nesting. **CVE-2026-31402**: In the Linux kernel, the following vulnerability has been resolved: nfsd: fix heap overflow in NFSv4.0 LOCK replay cache The NFSv4.0 replay cache uses a fixed 112-byte inline buffer (rp_ibuf[NFSD4_REPLAY_ISIZE]) to store encoded operation responses. This size was calculated based on OPEN responses and does not account for LOCK denied responses, which include the conflicting lock owner as a variable-length field up to 1024 bytes (NFS4_OPAQUE_LIMIT). When a LOCK operation is denied due to a conflict with an existing lock that has a large owner, nfsd4_encode_operation() copies the full encoded response into the undersized replay buffer via read_bytes_from_xdr_buf() with no bounds check. This results in a slab-out-of-bounds write of up to 944 bytes past the end of the buffer, corrupting adjacent heap memory. **CVE-2026-6100**: Use-after-free (UAF) was possible in the `lzma.LZMADecompressor`, `bz2.BZ2Decompressor`, and `gzip.GzipFile` when a memory allocation fails with a `MemoryError` and the decompression instance is re-used. This scenario can be triggered if the process is under memory pressure. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	QRadar versions 7.5.0 to 7.5.0 UP15 IF02
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7273957

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-3219, CVE-2025-30258, CVE-2023-50495, CVE-2025-1632, CVE-2025-5915, CVE-2025-5916, CVE-2025-5917, CVE-2025-5918, CVE-2023-32636, CVE-2025-3360, CVE-2025-4598, CVE-2025-23419, CVE-2025-5278, CVE-2025-5318, CVE-2025-5351, CVE-2025-5372, CVE-2025-5987, CVE-2025-8114, CVE-2022-27943, CVE-2022-41409, CVE-2023-4156, CVE-2024-0232, CVE-2024-13176, CVE-2025-13755, CVE-2025-4878, CVE-2024-11053, CVE-2024-7264, CVE-2024-9681, CVE-2025-36220, CVE-2025-36216, CVE-2025-36221, CVE-2026-28417, CVE-2026-28421, CVE-2026-33412, CVE-2006-10002, CVE-2026-4424, CVE-2026-5121, CVE-2026-1519, CVE-2026-35385, CVE-2026-35386, CVE-2026-35387, CVE-2026-35388, CVE-2026-35414, CVE-2026-27135, CVE-2024-56462, CVE-2026-34982, CVE-2024-41073, CVE-2025-40252, CVE-2025-68724, CVE-2026-23401, CVE-2026-31431, CVE-2026-4786, CVE-2026-35535, CVE-2025-68741, CVE-2026-23191)
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 systems. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Cloud Pak for Data System – Cyclops versions 11.3.0.2 – IFS IBM Db2 Server Edition versions 11.5.0 to 11.5.9 and 12.1.0 to 12.1.4 QRadar versions 7.5.0 to 7.5.0 UP15 IF02
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7272521 • https://www.ibm.com/support/pages/node/7273554 • https://www.ibm.com/support/pages/node/7272955 • https://www.ibm.com/support/pages/node/7273923 • https://www.ibm.com/support/pages/node/7272521 • https://www.ibm.com/support/pages/node/7273957

Affected Product	**Zyxel Networks**
Severity	**Medium**
Affected Vulnerability	Missing Authorization Vulnerability (CVE-2026-4795)
Description	Zyxel has released a security update addressing a vulnerability that exists in their products. **CVE-2026-4795**: A missing authorization vulnerability in the Zyxel GS1200v3 series switch firmware could allow a LAN-based unauthenticated attacker to read the system configuration from a log file via a crafted HTTP request. Zyxel advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	GS1200-5v3 versions 1.00(ACPS.2)C0 and earlier GS1200-8v3 versions 1.00(ACPT.2)C0 and earlier GS1200-5HPv3 versions 1.00(ACPU.2)C0 and earlier GS1200-8HPv3 versions 1.00(ACPV.2)C0 and earlier GS1200-10v3 versions 1.00(ACPW.2)C0 and earlier
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-missing-authorization-vulnerability-in-gs1200v3-series-switches-05-26-2026

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.