CET-SA-2026-001

Security fixes included in Inview Firmware 7.2.0

Advisory ID	CET-SA-2026-001
Product	Inview
Fixed firmware version	7.2.0
Affected firmware versions	Inview firmware versions prior to 7.2.0 may contain one or more of the affected third-party components listed in this advisory.
Publication date	2026-09-10
Severity	Multiple - depends on the individual vulnerability and product exposure. Published upstream severity ratings do not necessarily represent the effective severity in the context of the Inview product.
Status	Fixed
Related PCN	PCN # 20260622 Inview

1. Summary

Inview firmware 7.2.0 includes security updates for multiple third-party software components used by the embedded operating system. These updates address publicly disclosed vulnerabilities in network services, cryptographic libraries, system libraries, parsers and other supporting components.
The applicability and effective impact of an individual vulnerability depend on the component version, build options, Inview configuration, enabled services and deployment environment. Inclusion of a CVE in this advisory does not imply that every vulnerability is remotely exploitable on an Inview product.

2. Potential impact

Depending on the affected component and deployment conditions, the addressed vulnerabilities may affect availability, confidentiality, integrity, network-service robustness, processing of malformed or untrusted input, or cryptographic and secure-communication functions.
CE+T Power has not performed an individual product-level exploitability assessment for every upstream vulnerability listed in this advisory.

3. Remediation

CE+T Power recommends upgrading supported Inview systems to firmware version 7.2.0 or later in accordance with the applicable firmware update procedure. Where an immediate upgrade is not possible, Inview should remain deployed according to CE+T Power network-security recommendations, with network access restricted to trusted networks and authorised users.

4. Addressed third-party security vulnerabilities

The following security references were addressed through third-party component updates included in Inview firmware 7.2.0. References are consolidated by component; duplicate entries from the release-maintenance records are shown only once.

Component	Security references addressed

Component	Security references addressed
BIND	CVE-2026-3039, CVE-2026-3592, CVE-2026-5946, CVE-2026-5950, CVE-2026-1519, CVE-2025-13878, ISC BIND issue 5751, ISC BIND issue 5817, ISC BIND issue 5800, ISC BIND issue 5826
dnsmasq	CVE-2026-2291, CVE-2026-4890, CVE-2026-4891, CVE-2026-4892, CVE-2026-4893, CVE-2026-5172
Expat	CVE-2026-45186, CVE-2026-7210, CVE-2026-41080, CVE-2026-32776, CVE-2026-32777, CVE-2026-32778, CVE-2026-24515, CVE-2026-25210
glibc	CVE-2026-4046, CVE-2026-4437, CVE-2026-4438, CVE-2026-5450, CVE-2026-5928, CVE-2025-15281, CVE-2026-0861, CVE-2026-0915
haveged	CVE-2026-41054
ImageMagick	CVE-2026-42326, CVE-2026-45031, CVE-2026-45358, CVE-2026-45359, CVE-2026-45624, CVE-2026-45664, CVE-2026-46520, CVE-2026-46521, CVE-2026-46522, CVE-2026-46523, CVE-2026-46557, CVE-2026-46559, CVE-2026-28493, CVE-2026-28494, CVE-2026-28686, CVE-2026-28687, CVE-2026-28688, CVE-2026-28689, CVE-2026-28690, CVE-2026-28691, CVE-2026-28692, CVE-2026-28693, CVE-2026-30883, CVE-2026-30929, CVE-2026-30931, CVE-2026-30935, CVE-2026-30936, CVE-2026-30937, CVE-2026-31853, CVE-2026-32259, CVE-2026-32636, CVE-2026-33535, CVE-2026-33536, CVE-2026-33899, CVE-2026-33900, CVE-2026-33901, CVE-2026-33902, CVE-2026-33905, CVE-2026-33908, CVE-2026-34238, CVE-2026-40169, CVE-2026-40183, CVE-2026-40310, CVE-2026-40311, CVE-2026-40312, CVE-2026-22770, CVE-2026-23874, CVE-2026-23876, CVE-2026-24481, CVE-2026-25638, CVE-2026-25794, CVE-2026-25795, CVE-2026-25796, CVE-2026-25798, CVE-2026-25799, CVE-2026-25897, CVE-2026-25989, CVE-2026-26066, CVE-2026-26283, CVE-2026-26284, CVE-2026-26983, CVE-2025-66628
libgpg-error	T8239
libssh2	CVE-2026-7598
libusb	CVE-2026-23679, CVE-2026-47104
OpenSSH	CVE-2025-61984, CVE-2025-61985, CVE-2026-35385, CVE-2026-35386, CVE-2026-35387, CVE-2026-35388, CVE-2026-35414
python-urllib3	CVE-2026-44431, CVE-2026-44432, CVE-2026-21441
Python 3	CVE-2026-3276, CVE-2026-7774, CVE-2026-8328, CVE-2024-6923, CVE-2025-13836, CVE-2025-59375
sed	CVE-2026-5958
unzip	CVE-2021-4217
FreeType	CVE-2026-23865
giflib	CVE-2021-40633, CVE-2025-31344, CVE-2026-23868
GnuTLS	CVE-2026-33845, CVE-2026-33846, CVE-2026-3832, CVE-2026-3833, CVE-2026-42009, CVE-2026-42010, CVE-2026-42011, CVE-2026-42012, CVE-2026-42013, CVE-2026-42014, CVE-2026-42015, CVE-2026-5260, CVE-2026-5419, CVE-2025-14831, CVE-2026-1584, CVE-2025-9820
libcap	CVE-2026-4878
libcurl	CVE-2026-7168, CVE-2026-7009, CVE-2026-6429, CVE-2026-6276, CVE-2026-6253, CVE-2026-5773, CVE-2026-5545, CVE-2026-4873, CVE-2026-3805, CVE-2026-3784, CVE-2026-3783, CVE-2026-1965, CVE-2025-13034, CVE-2025-14017, CVE-2025-14524, CVE-2025-14819, CVE-2025-15079, CVE-2025-15224
libpcap	CVE-2025-11961
libxml2	CVE-2026-6732, CVE-2026-1757, CVE-2026-0990, CVE-2026-0992, CVE-2025-10911, CVE-2026-0989
python-pyasn1	CVE-2026-30922
python-requests	CVE-2026-25645

Component	Security references addressed
SQLite	CVE-2025-70873
systemd	CVE-2026-40226
util-linux	CVE-2026-27456
xz	CVE-2025-31115, CVE-2026-34743
OpenSSL	CVE-2025-9230, CVE-2025-9231, CVE-2025-9232, CVE-2025-4575, CVE-2025-11187, CVE-2025-15467, CVE-2025-15468, CVE-2025-15469, CVE-2025-66199, CVE-2025-68160, CVE-2025-69418, CVE-2025-69419, CVE-2025-69420, CVE-2025-69421, CVE-2026-22795, CVE-2026-22796, CVE-2026-31790, CVE-2026-2673, CVE-2026-28387, CVE-2026-28388, CVE-2026-28389, CVE-2026-28390, CVE-2026-31789
libpng	CVE-2026-33416, CVE-2026-33636, CVE-2026-34757, GHSA-6fr7-g8h7-v645, CVE-2026-22695, CVE-2026-22801, CVE-2026-25646, CVE-2025-66293, CVE-2025-64505, CVE-2025-64506, CVE-2025-64720, CVE-2025-65018
libssh	CVE-2025-14821, CVE-2026-0964, CVE-2026-0965, CVE-2026-0966, CVE-2026-0967, CVE-2026-0968
Net-SNMP	CVE-2025-68615
BusyBox	CVE-2025-46394, CVE-2025-60876
libtasn1	CVE-2025-13151
Vim	CVE-2025-66476
libxslt	CVE-2025-7424, CVE-2025-9714, CVE-2025-11731

5. Assessed vulnerabilities not affecting Inview

During the security review performed for Inview firmware 7.2.0, CE+T Power assessed CVE-2026-31431 (“Copy Fail”). Based on the Linux kernel version and mitigations already present in the Inview platform, CE+T Power concluded that Inview is not affected by this vulnerability.

CVE	Assessment	Rationale
CVE-2026-31431	Not affected	Required kernel mitigation already present in the Inview platform

6. Additional information

For technical assistance with firmware updates, installation, configuration or product operation, please use the CE+T Power technical support portal:

CE+T Power Technical Support

To report a suspected cybersecurity vulnerability or security incident affecting a CE+T Power product, contact cybersecurity@cet-power.com. This address is dedicated to vulnerability and security-incident reporting and is not a technical-support contact.

cybersecurity@cet-power.com