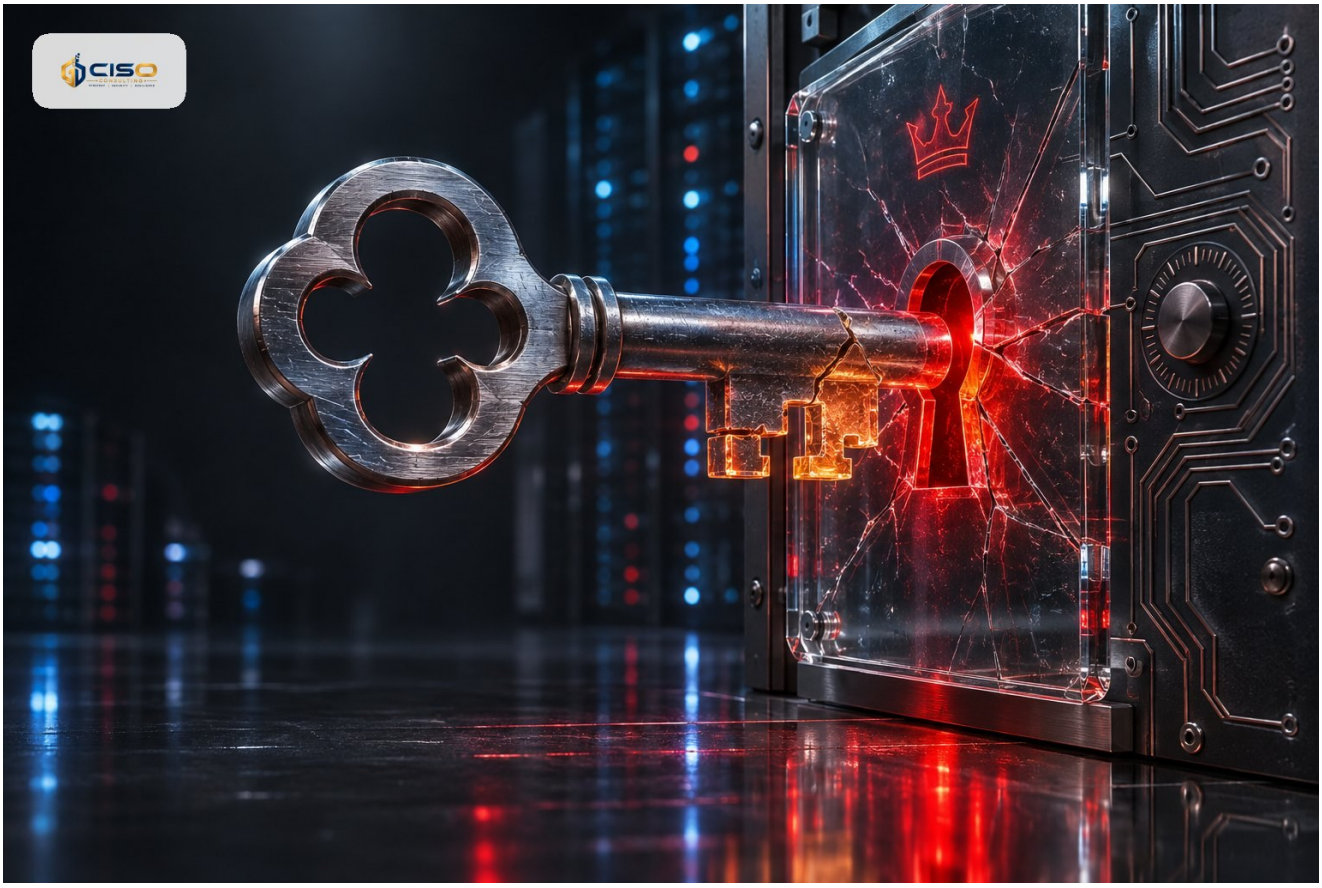
ASUS patches critical hard-coded key flaws in Control Center Express



ASUS released Control Center Express v1.7.29 to fix three critical flaws, including CVE-2026-114202 (CVSS 10.0), which lets an unauthenticated remote attacker forge a token and gain administrator access. Related products were also patched.

- Three critical flaws are fixed in Control Center Express v1.7.29: CVE-2026-114202, CVE-2026-114204 and CVE-2026-114205.
- CVE-2026-114202 (CVSS 10.0) stems from a hard-coded cryptographic key and needs no privileges or user interaction.
- CVE-2026-114204 allows forging a session token for a recently logged-in account; CVE-2026-114205 lets a low-privileged user create an administrator account.
- ASUS says versions before v1.7.29 are affected, but the CVE records list only up to v1.7.27, so

> v1.7.28 is unclear.
>
> - Control Center Enterprise, Control Center Datacenter and Armoury Crate also received fixes, including critical CVE-2026-126574.

ASUS has released Control Center Express v1.7.29 to address three critical vulnerabilities that could allow remote attackers to take administrative control of the management console and the devices it manages.

What was fixed

The most serious is CVE-2026-114202, rated CVSS 10.0. It arises from a hard-coded cryptographic key and allows an unauthenticated remote attacker to forge an authentication token and obtain administrator privileges, with no user interaction.

CVE-2026-114204 is also a hard-coded key problem. It lets a low-privileged remote attacker forge a session token for a recently logged-in account. CVE-2026-114205 is an authorization flaw that lets a low-privileged user create an administrator account.

Control Center Express is a central dashboard used by IT administrators to monitor and remotely manage fleets of PCs. ASUS markets it to businesses and IT service providers.

Scope and version uncertainty

ASUS's bulletin says versions earlier than v1.7.29 are affected. The CVE records, however, list affected versions only through v1.7.27, so the status of v1.7.28 is unclear. Treating v1.7.28 as affected is the cautious reading.

Other ASUS updates

ASUS also patched CVE-2026-126574, a critical flaw that lets a user with the low-privileged Viewer role change an administrator's password. It affects Control Center Datacenter 4.0.0.2 and earlier and Control Center Enterprise 3.1.0.8 and earlier. Armoury Crate was updated for CVE-2026-112115, a high-severity local privilege escalation affecting versions up to and including 6.7.2.

The source does not mention active exploitation.

What to do now

1. Inventory where ASUS Control Center Express, Control Center Enterprise, Control Center Datacenter and Armoury Crate are deployed.
2. Upgrade Control Center Express to v1.7.29, including v1.7.28 installations, then update agents on managed devices via Select Function → Client Agent Updater and verify versions.
3. Apply the vendor updates for Control Center Enterprise, Control Center Datacenter and Armoury Crate.

4. Until patched, restrict network access to the management console to trusted administrative networks.
5. Review administrator accounts and recent password changes on these consoles for unexpected creation or modification.
6. Record the remediation under your vulnerability and patch management process for NCA ECC and SAMA CSF evidence.