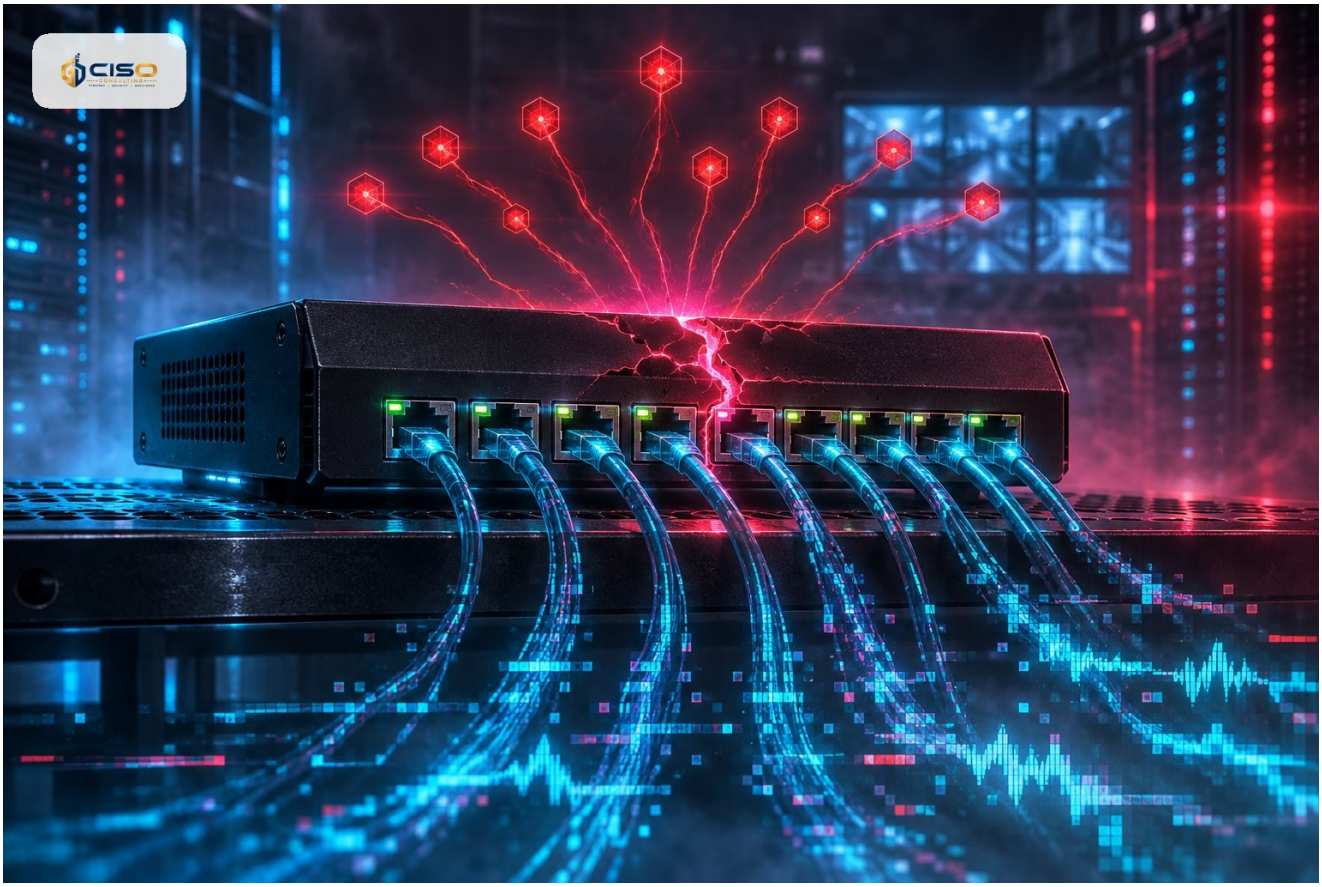
CISA flags critical flaws in Kiloview E3 NDI Encoder firmware before 1.30



CISA has published an advisory on Kiloview E3 NDI Encoder firmware older than 1.30. Nine CVEs could let an attacker fully compromise the device, with a vendor CVSS v3 score of 9.9.

- Affected: Kiloview E3 firmware versions earlier than 1.30.
- Nine CVEs are listed, from CVE-2026-109122 to CVE-2026-110825.
- Weakness types include OS command injection, missing authentication for a critical function, insufficient session expiration, path traversal, NULL pointer dereference and hard-coded credentials.
- Successful exploitation could allow full compromise of the device; the CVSS v3 score is 9.9.
- CISA lists the sectors as Communications and Information Technology, with worldwide deployment.

What was published

CISA has issued an industrial control systems advisory covering the Kiloview E3 NDI Encoder. The affected product is E3 firmware earlier than version 1.30. The advisory lists nine CVEs and a vendor CVSS v3 score of 9.9.

The weaknesses fall into six categories: **OS command injection**, missing authentication for a critical function, insufficient session expiration, path traversal, NULL pointer dereference and use of hard-coded credentials. According to CISA, successful exploitation could allow an attacker to fully compromise the device.

One of the listed issues, CVE-2026-109122, concerns the network management service. It does not properly sanitize a field used when static routes are configured through the web management API, so an authenticated user with route-configuration permission could run commands.

Why it matters

CISA associates the product with the Communications and Information Technology sectors and notes worldwide deployment. The vendor is headquartered in China. Organizations that use these encoders in media, broadcast, conferencing or internal video environments should confirm whether any E3 units are present on their networks.

What to do next

Start with an inventory of Kiloview E3 devices and their firmware versions. Then consult the full CISA advisory and the vendor's guidance for the fixed release and any further mitigation steps, as the source excerpt does not detail them. Until units are updated, limit who can reach their management interfaces.

What to do now

1. Inventory all Kiloview E3 NDI Encoder units and record their firmware versions.
2. Plan and test an update to firmware 1.30 or later, following the vendor's guidance and the full CISA advisory.
3. Restrict access to device management interfaces to a dedicated management network and authorized administrators.
4. Review accounts with route-configuration permission and change any default or shared credentials.
5. Monitor these devices for unexpected configuration changes or unusual outbound connections.