AutomationDirect C-More EA9 Programming Software: Heap Overflow Flaw Triggered by Malicious Project Files



CISA reports CVE-2026-127280 in C-More EA9 Programming Software up to V6.80. A crafted project file can corrupt memory and may lead to code execution. CVSS v3 is 7.8.

- Affected: C-More EA9 Programming Software version V6.80 and earlier.
- CVE-2026-127280 is a heap-based buffer overflow with a CVSS v3 score of 7.8.
- The application does not properly validate data read from a project file before using it in heap memory operations.
- Exploitation requires a user to open a malicious project file, which may arrive by email, file sharing or removable media.
- Impact ranges from instability or a crash to potential arbitrary code execution.

CISA has published an industrial control systems advisory on a vulnerability in AutomationDirect's C-More EA9 Programming Software, affecting version V6.80 and earlier. The issue is tracked as CVE-2026-127280 and carries a CVSS v3 score of 7.8.

What the flaw is

The software does not adequately validate data it reads from a project file before using that data in heap memory operations. A specially crafted file can cause a heap buffer overrun when the file is opened, corrupting memory and destabilizing the application. CISA notes this could lead to a crash and potentially arbitrary code execution.

Exploitation depends on user interaction: an attacker must convince someone to open a malicious project file. The advisory names common delivery routes such as email, file sharing and removable media.

Why it matters

CISA lists the affected product's sectors as Critical Manufacturing, Energy, and Water and Wastewater Systems, with deployment worldwide. Organizations in the Kingdom that run operational technology in these areas, or that use engineering workstations with this tool, should check whether it is present in their environment.

The excerpt we reviewed does not describe a vendor fix or specific mitigations, so teams should consult the full CISA advisory and the vendor for remediation guidance.

Recommended approach

Because the attack relies on a file being opened, controls over how project files reach engineering workstations are the practical first line of defense, alongside confirming versions and following the vendor's guidance.

What to do now

1. Inventory engineering workstations and identify any with C-More EA9 Programming Software V6.80 or earlier.
2. Review the full CISA advisory and contact AutomationDirect for fix or mitigation guidance.
3. Open project files only from trusted, verified sources, and treat unexpected files received by email or file sharing as suspect.
4. Restrict and scan removable media used on engineering workstations.
5. Alert OT engineers and maintenance contractors to this file-based risk.