CISA Flags Vulnerabilities in Dorsett Controls InfoScan Used in Water Systems



CISA published an ICS advisory on Dorsett Controls InfoScan versions up to 1.45.0, covering six CVEs. Exploitation could expose data and credentials or allow network traffic to be intercepted and altered.

- Affected: Dorsett Controls InfoScan version 1.45.0 and earlier.
- Six CVEs are listed, from CVE-2026-117659 to CVE-2026-120298.
- The CVSS v3 score given is 8.1.
- Weakness types include improper certificate validation, a hard-coded cryptographic key and missing authentication for a critical function.
- The advisory lists Water and Wastewater Systems as the affected sector, with worldwide deployment.

CISA has released an industrial control systems advisory for InfoScan, a product from Dorsett Controls, a company headquartered in the United States. The advisory covers InfoScan versions up to and including 1.45.0 and lists six CVEs.

What the advisory says

According to the advisory, successful exploitation could let an attacker retrieve sensitive system information, access application data without authorization, recover stored credentials, or intercept and manipulate network communications. The CVSS v3 score given is 8.1.

The weakness categories named include improper certificate validation, exposure of sensitive system information to an unauthorized control sphere, use of a hard-coded cryptographic key, missing authentication for a critical function, and error messages that contain sensitive information. One example described is the InfoScan Electron desktop client accepting TLS certificates without checking whether they can be trusted.

The advisory identifies Water and Wastewater Systems as the critical infrastructure sector concerned, with the product deployed worldwide.

What to do next

The excerpt we reviewed does not include vendor fixes or mitigation steps. Operators should read the full CISA advisory and any vendor guidance before deciding on remediation. In the meantime, confirm whether InfoScan is present in your environment and which version runs, and review how the clients and servers are exposed on the network.

What to do now

1. Check asset inventories for InfoScan and record the installed versions.
2. Read the full CISA advisory and any Dorsett Controls guidance for fixes or mitigations.
3. Restrict network access to InfoScan systems and keep them segmented from corporate networks.
4. Treat credentials stored or used by InfoScan as potentially exposed and plan rotation if affected versions are found.
5. Monitor for unusual network activity involving InfoScan hosts.