

CISA issues advisory for multiple vulnerabilities in Malcolm network analysis platform



CISA has published an advisory detailing multiple security vulnerabilities in its Malcolm network traffic analysis platform, including cross-site scripting, command injection, and authentication bypass flaws.

- CISA Malcolm network analysis platform contains multiple security vulnerabilities with a CVSS score of 8.8
- Identified flaws include cross-site scripting, OS command injection, path traversal, and server-side request forgery
- Additional vulnerabilities involve authentication bypass, missing authorization, use of default credentials, and improper certificate validation
- The platform is deployed worldwide and affects critical infrastructure sectors including energy, IT,

and water systems

- At least one vulnerability (CVE-2026-90443) does not require authentication to exploit

Multiple vulnerabilities identified

The US Cybersecurity and Infrastructure Security Agency has released an industrial control systems advisory detailing multiple security vulnerabilities in **CISA Malcolm**, a network traffic analysis platform. The vulnerabilities carry a combined CVSS v3 score of 8.8, indicating high severity. The flaws span a wide range of security weaknesses including improper input neutralization leading to cross-site scripting, OS command injection, and path traversal attacks.

Additional vulnerabilities include server-side request forgery, authentication bypass through spoofing, missing authorization controls, and missing authentication for critical functions. The advisory also identifies issues with incorrect authorization, use of default credentials, improper certificate validation, URL redirection to untrusted sites, and dependencies on vulnerable third-party components. Notably, CVE-2026-90443 involves a web interface that reflects portions of request URLs into script contexts without adequate encoding and does not require authentication to access.

Deployment and impact scope

Malcolm is deployed worldwide and affects critical infrastructure sectors including energy, information technology, and water and wastewater systems. The platform's use in operational technology environments and critical infrastructure monitoring makes these vulnerabilities particularly significant for organizations relying on the tool for network visibility and security analysis.

Risk considerations for Saudi institutions

Regulated institutions in the Kingdom using Malcolm for network analysis or security monitoring should assess their exposure immediately. The combination of authentication bypass vulnerabilities and the platform's potential deployment in critical infrastructure environments creates elevated risk for unauthorized access and system compromise.

What to do now

1. Identify all deployments of CISA Malcolm within your network infrastructure and operational technology environments
2. Review access logs for Malcolm instances to detect any suspicious activity or unauthorized access attempts
3. Implement network segmentation to isolate Malcolm deployments from critical systems until patches are applied

4. Monitor CISA advisories for vendor patches and remediation guidance specific to the identified CVE numbers
5. Assess whether Malcolm is used in any critical infrastructure monitoring capacity and evaluate alternative solutions if immediate patching is not feasible
6. Document Malcolm usage and vulnerability exposure as part of your risk register and report to relevant governance committees