CISA flags cleartext transmission weakness in InterSystems IRIS for Health



CISA published a medical advisory on InterSystems IRIS for Health, where TLS/SSL is off by default. An attacker could view transmitted data and use it to log in. The CVSS v3 score is 8.1.

- CVE-2026-111594 concerns cleartext transmission of sensitive information.
- TLS/SSL encryption is turned off by default in InterSystems IRIS for Health.
- An attacker could view transmitted data and use it to log into the device.
- Listed versions: 2026.2.0.221, 2026.1.0.235 and 2025.3.0.226.
- The vendor recommends configuring the IRIS superserver to require SSL/TLS.

CISA has released a medical advisory covering InterSystems IRIS for Health, a product used in the Healthcare

and Public Health sector and deployed worldwide. The vendor is headquartered in the United States.

What the issue is

The advisory tracks CVE-2026-111594, classed as cleartext transmission of sensitive information. In IRIS for Health, TLS/SSL encryption is turned off by default. As a result, an attacker able to observe traffic could view transmitted data and use it to log into the device. The advisory gives a CVSS v3 base score of 8.1.

The versions listed are InterSystems IRIS for Health 2026.2.0.221, 2026.1.0.235 and 2025.3.0.226.

Recommended mitigation

InterSystems recommends that users configure the IRIS superserver to require SSL/TLS. The vendor's documentation, linked from the CISA advisory, describes how to do this. The source does not mention a patched version or reports of exploitation.

What this means for institutions

Because the weakness stems from a default setting, deployments may be exposed even when no software flaw in the usual sense is present. Healthcare providers and any institution running IRIS for Health should confirm how their instances are configured rather than assume encryption is active.

What to do now

1. Inventory all InterSystems IRIS for Health instances and note their versions.
2. Check whether the IRIS superserver currently requires SSL/TLS on each instance.
3. Configure the superserver to require SSL/TLS following the vendor's documentation.
4. Test client and integration connections after enabling encryption to avoid service disruption.
5. Review access logs and rotate credentials where cleartext exposure on the network is possible.