Thermo Fisher Torrent Suite Software: Path Traversal Flaw Allows File Reads



CISA reports a path traversal flaw (CVE-2026-107777) in Torrent Suite Software 5.18 and earlier. An authenticated attacker could read files on the Torrent Server. Thermo Fisher advises updating to 5.22 or later.

- Affected: Torrent Suite Software version 5.18 and earlier.
- CVE-2026-107777 is a path traversal flaw (CWE-22) with a CVSS v3 score of 6.5.
- An authenticated attacker could read arbitrary files on the Torrent Server that the web service account can access.
- Thermo Fisher has fixed the issue in version 5.22 and later.
- CISA lists the Healthcare and Public Health sector, with worldwide deployment.

CISA has published a medical advisory on Thermo Fisher Torrent Suite Software, covering a path traversal vulnerability tracked as CVE-2026-107777.

What is affected

The flaw affects Torrent Suite Software version 5.18 and earlier. The product improperly restricts pathnames to a permitted directory (CWE-22). The CVSS v3 score is 6.5. CISA lists the Healthcare and Public Health sector and notes worldwide deployment.

Impact

An attacker who is already authenticated could read arbitrary files on the Torrent Server. Exposure is limited to files that the web service account can access. The source does not mention active exploitation.

Fix and next steps

Thermo Fisher has fixed the vulnerability and recommends updating to Torrent Suite Software 5.22 or later. The vendor's security bulletin carries further mitigation detail.

Institutions that run this software, such as laboratories and healthcare or research organisations, should confirm their version, plan the update, and review who holds accounts on the server. Because exploitation requires authentication, tight account control reduces exposure while the update is scheduled.

What to do now

1. Identify any Torrent Suite Software instances and record their versions.
2. Update instances at version 5.18 or earlier to 5.22 or later.
3. Review Thermo Fisher's security bulletin for additional mitigation guidance.
4. Audit and limit user accounts that can authenticate to the Torrent Server.
5. Check what files the web service account can reach and reduce unnecessary access.