

# Security Bulletin

## SUMMARY

**CVE:** Privileged Escalation Vulnerability on the Torrent Suite™ Dx software

<b>PUBLISHED DATE:</b> MAY 15, 2026	<b>CVE NUMBER:</b> CVE-2026-41085	<b>CVSS V4.0 SCORE:</b> 9.3	<b>SEVERITY:</b> Critical
--	--------------------------------------	--------------------------------	------------------------------

## DESCRIPTION

Thermo Fisher Scientific has identified a security vulnerability in the Torrent Suite™ Dx software through routine penetration testing. The vulnerability may allow an authenticated user with limited privileges to potentially escalate access to administrator-level permissions through specific system interfaces. If exploited, this could enable unauthorized modification of system settings, configurations, software or data on the instrument.

## SOLUTION

Thermo Fisher Scientific is committed to maintaining the security and integrity of its products and will provide additional information as it becomes available.

Please contact your local Thermo Fisher Scientific Field Support team for any additional questions or contact [product.security@thermofisher.com](mailto:product.security@thermofisher.com) for any questions related to the vulnerabilities.

**Table 1. Impacted products**

Product	Affected versions
Torrent Suite™ Dx software	The security vulnerability affects versions 5.14.2 and earlier.

**Table 2. Remediation plan**

Product	Remediation plan
Torrent Suite™ Dx software	<p>Thermo Fisher Scientific has developed a security update to address this vulnerability. To implement this update:</p> <ul style="list-style-type: none"> <li>• Systems running version 5.14.2 can receive the security update.</li> <li>• Systems running versions earlier than 5.14.2 must first be upgraded, and then the security update can be applied.</li> </ul> <p>Customers should contact their local Field Support representative to schedule the required update.</p>