

Security Bulletin

SUMMARY

Mitigating Vulnerabilities in Torrent Suite™ Dx Software

PUBLISHED DATE:
OCTOBER 26, 2026

SEVERITY:
High

DESCRIPTION

Thermo Fisher Scientific has identified security vulnerabilities through a routine internal security review impacting Torrent Suite™ Dx Software used in connection with the Ion PGM™ Dx system (see Table 1 and Table 2). The identified vulnerabilities include improper authorization, operating system command injection and path traversal that could allow an unauthorized user to interfere with certain software settings or workflow functions, potentially impacting integrity of the results.

At this time, Thermo Fisher Scientific has no evidence to indicate that these vulnerabilities have been exploited.

SOLUTION

Our team is developing a security update for the impacted software and will make it available to customers after the update completes the appropriate regulatory review and validation process. While the update is being finalized, Thermo Fisher Scientific recommends the following measures to help reduce the risk (see Table 3).

Please contact your local Thermo Fisher Scientific support representative for any additional questions or contact product.security@thermofisher.com for any questions related to the vulnerability.

Thermo Fisher Scientific is committed to maintaining the security, integrity and reliability of our products. We appreciate your partnership and recommend implementing the applicable updates as soon as practical.

Table 1. List of vulnerabilities

Description	CVSS Score
Improper Authorization in Administrator Account Management	8.7
Command Injection via Reference Metadata and FASTA File Processing	8.7
Improper Authorization in Report and Quality Control Functions	7.2
Path Traversal in Archive Extraction	7.2

Table 2. Impacted products

Product	Affected Versions
Torrent Suite Dx software	These security vulnerabilities affect versions 5.14.2 and earlier.

Table 3. Remediation plan

Product	Remediation plan
Torrent Suite Dx software	1. Restrict access to authorized personnel only. Because exploiting these vulnerabilities requires access to the local network, limiting access helps reduce the risk of unauthorized activity. 2. Confirm the PGM Dx instrument and any associated systems are not directly accessible from the public Internet and are protected by appropriate network security controls, such as firewalls or network segmentation. 3. Continue monitoring connected systems for unexpected connections or other unusual network activity so that any potential issues can be identified and investigated promptly.