

Security Bulletin

SUMMARY

Mitigating Vulnerabilities in Ion Torrent™ Genexus™ Dx and Assay Development Software

PUBLISHED DATE:
AUGUST 13, 2026

SEVERITY:
Critical

DESCRIPTION

Thermo Fisher Scientific has identified security vulnerabilities in Ion Torrent™ Genexus™ Dx Software version 6.8.2.1 and 6.8.4.0 and Assay Development Software versions 6.8.4.0 and 7.0.2 through a routine internal security review (see Table 1 and Table 2). The identified vulnerabilities could allow an unauthorized user to interfere with certain software settings or workflow functions.

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

SOLUTION

Our team has developed a security update for Ion Torrent™ Genexus™ Dx software version 6.8.2.1 and 6.8.4.0 and will make it available to customers after the update completes the appropriate regulatory review process. While the update is being finalized, we recommend the following measures to help reduce the risk (see Table 3).

Thermo Fisher Scientific advises customers using the impacted versions of Ion Torrent™ Genexus™ Dx and Assay Development Software plan to upgrade to Ion Torrent™ Genexus™ Dx Software version 6.8.2.2 or 6.8.4.1 and Ion Torrent™ Genexus™ Assay Development Software version 6.8.4.1 or 7.0.2.1, when they become available.

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

Note: Once the CVE IDs are shared, we will provide an update to this table.

Description	CVSS Score
Privileged Account Takeover Through Weak Password Recovery and Improper Authorization	9.5
Privileged Escalation Through Authenticated OS Command Injection in QIIME and Reference Genome Upload Workflows	9.4
Missing Authentication on Installer and Reporting Callback APIs	9.2
Improper Authorization in Result-Review Mutation APIs	7.0

Table 2. Impacted products

Product	Affected Versions
Ion Torrent™ Genexus™ Dx software	These security vulnerabilities affect version 6.8.2.1 and 6.8.4.0 and earlier.
Ion Torrent™ Genexus™ Assay Development software	These security vulnerabilities affect version 6.8.4.0 and 7.0.2 and earlier.

Product	Mitigating Controls
Ion Torrent™ Genexus™ Dx and Assay Development 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 Genexus™ 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.