Security Bulletin

SUMMARY

CVE: Credential Vulnerability in Thermo Scientific™ ePort software

PUBLISHED DATE:	CVE NUMBER:	CVSS 3.1 SCORE:	SEVERITY:
AUGUST 18, 2025	CVE-2025-32992	8.5	High

DESCRIPTION

Thermo Fisher Scientific has released a security update for the ePort software. This update resolves a hardcoded credential vulnerability that can allow remote access to the file system, potentially impacting data integrity and/or network resiliency.

SOLUTION

Thermo Fisher Scientific has developed the following remediation plan to address this vulnerability (see Table 2).

Please use the link here to contact Technical Support for any additional support or contact product.security@thermofisher.com for any questions related to the vulnerability.

ACKNOWLEDGEMENTS

Thermo Fisher Scientific would like to thank the Bugcrowd researcher 'orosec' for their identification of the vulnerability covered in this security bulletin.

EXTERNAL REFERENCES

https://www.thermofisher.com/order/catalog/product/TEOM1405

Table 1. Affected software

Product	Related affected products
ePort software	The security vulnerability impacts version 3.0.0 and earlier of the ePort software when using the Thermo Scientific 1405 TEOM™ Continuous Ambient Particulate Monitor instrument. *ePort software version 4.1.0 and greater along with their compatible instruments are not impacted by this vulnerability.

Table 2. Security updates to address this vulnerability

Product	Remediation plan
ePort software	Thermo Fisher Scientific has developed an update to mitigate the risk of this vulnerability for Thermo Scientific 1405 TEOM™ Continuous Ambient Particulate Monitor instrument customers. A Thermo Fisher Scientific Support Engineer will contact potentially impacted customers with more information about applying the update.