Security Bulletin

SUMMARY

CVE: Impact of Multiple Vulnerabilities in Kubernetes Ingress NGINX Controller on Thermo Scientific™ software

PUBLISHED DATE:	CVE NUMBERS:	CVSS 3.1 SCORE:	SEVERITY:
May 15, 2025	CVE-2025-1097, CVE-2025-1098, CVE-2025-1974, CVE-2025-24513 & CVE-2025-24514	9.8 (CVE-2025-1974), 8.8 (CVE-2025-1097, CVE-2025-1098, CVE-2025-24514) & 4.4 (CVE-2025-24513)	Critical

DESCRIPTION

Thermo Fisher Scientific is aware of the recent security vulnerabilities published in the Ingress NGINX Controller for Kubernetes. Discovered by Wiz Research, the vulnerabilities within the ingress NGINX controller could allow for unauthenticated remote code execution, potentially leading to unauthorized access across containers and resulting in a full cluster takeover.

Thermo Fisher Scientific promptly launched an investigation to identify products potentially affected by this issue and discovered the following software subject to these vulnerabilities:

SOLUTION

Thermo Fisher Scientific has released the following security updates to address this vulnerability (see Table 2).

For any questions related to the vulnerability, please contact **product.security@thermofisher.com**.

EXTERNAL REFERENCES

https://www.wiz.io/blog/ingress-nginx-kubernetes-vulnerabilities#what-is-ingress-nginx-controller-for-kubernetes-5.

Table 1. Affected software

Product	Related affected products
Software Delivery Platform (SDP)	All software installations that require SDP version 4.0 and earlier. Please contact your account manager for more information about whether your products have SDP installed.
Ardia™ Platform	This vulnerability impacts publicly accessible configurations of Ardia Platform v1.0 and v1.1. Default configurations of the Ardia Platform are not impacted.

Table 2. Security updates to address this vulnerability

Product	Remediation steps
Software Delivery Platform (SDP)	Thermo Fisher Scientific has released SDP version 4.1 to address this vulnerability, which is included as the default installation for new customers. For existing customers running an impacted version of SDP, a Thermo Fisher Scientific Service Engineer must perform the update on-site. Please contact your dedicated Service Engineer or use the link here to contact Technical Support to schedule your on-site visit. Thermo Fisher Scientific recommends that customers do not make any changes to the standard SDP configuration.
Ardia Platform	Thermo Fisher Scientific has released an update for Ardia Platform v1.1 to address this vulnerability. Please use the Thermo Fisher Scientific Digital Science Support Resource Center website to download the software update. **Note:** *Login is required to access the Thermo Fisher Scientific Digitial Science Support Resource Center.* Thermo Fisher Scientific recommends customers apply the following supplemental mitigations: • Upgrade to the patched version of Ardia v1.1 if running Ardia v1.0 • Use the standard Ardia configuration • Take their environment offline if configured to be publicly accessible