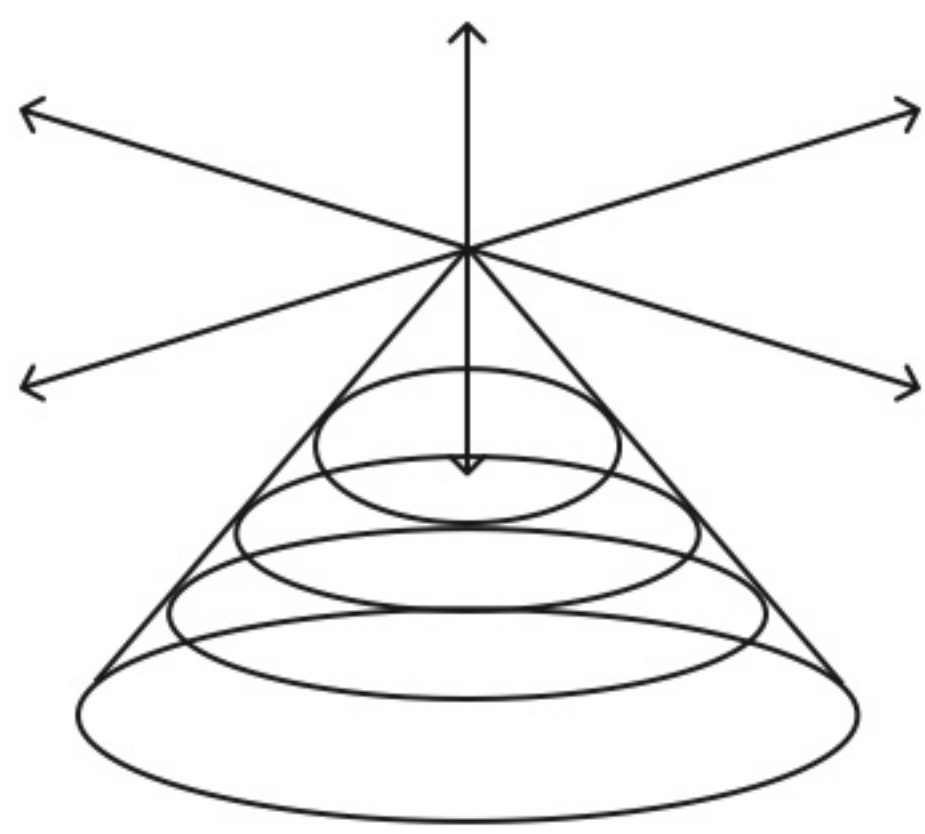




Foundation Models

A global model that combines real-time internet exploitation telemetry with EPSS and monitors over 18,000+ exploited CVEs to help you prioritize and remediate threats.

Our Foundation Models API delivers best in the industry efficiency across coverage levels.

Get real-time CVE updates

We offer a robust UI and API for data discovery. Our CVE database updates hourly.

Run and save searches

Find CVEs by score thresholds, recent score changes, exploitation activity, products, vendors, and more.

Explore model thresholds

Change threshold parameters to filter the data page for better prioritization.

Track model performance

View vulns distributed by score, compare models over time, and view curated lists of CVEs by Known Exploitation Activity.

Global Model (30 days ago)

3 Months Ago
8,807
Known Exploitation Activity

1 Year Ago
11,809
Known Exploitation Activity

Over a Year ago
16,512
Known Exploitation Activity

empiricalsecurity.com

app.empiralsecurity.com/search?page=55&q=exploitation_activity%3A0-7

Global Model Global Data Your Data Models Insights Agent Search CVEs...

exploitation_activity:0-7

Threshold 0-100 Scores

New Activity 22 Known Exploitation Activity

1 Week Ago 6,779 Known Exploitation Activity

1 Month Ago 6,520 Known Exploitation Activity

3 Months Ago 6,574 Known Exploitation Activity

1 Year Ago 6,554 Known Exploitation Activity

Over a Year ago 6,234 Known Exploitation Activity

6 Queries

6,779 Results Actions 55 of 339

SHARED	Empirical Score	CVE ID
All Vulns	97.1% Top 1%	CVE-2018-7665
Redhat	97.1% Top 1%	CVE-2025-24514
Critical and High	97.1% Top 1%	CVE-2025-31161
Wordpress	97.1% Top 1%	CVE-2021-42287
Remote Code Execution	97.1% Top 1%	CVE-2024-54085
CVSS 7+, Empirical 1+	97.1% Top 1%	CVE-2009-1031
PRIVATE	97.1% Top 1%	CVE-2018-0258
	97.1% Top 1%	CVE-2016-0101
	97.1% Top 1%	CVE-2018-11784
	97.1% Top 1%	CVE-2023-37470
	97.1% Top 1%	CVE-2025-11371
	97.1% Top 1%	CVE-2025-57819
	97.1% Top 1%	CVE-2025-48827
	97.1% Top 1%	CVE-2019-17571
	97.1% Top 1%	CVE-2023-28341
	97.1% Top 1%	CVE-2023-33831
	97.1% Top 1%	CVE-2022-4068

CVE-2025-24514

Details Remediations Exploit Code Chatter Malware

Summary

A security issue was discovered in ingress-nginx where the 'auth-url' Ingress annotation can be used to inject configuration into nginx. This can lead to arbitrary code execution in the context of the ingress-nginx controller, and disclosure of Secrets accessible to the controller. (Note that in the default installation, the controller can access all Secrets cluster-wide.)

Critical Indicators

Chatter	Exploit Code
Exploitation	References
Threat Intel	Vendor
Vuln Attributes	

Known Exploitation Activity

Last Known: Mar 28, 2026 2 Known Sources 1W 1M 3M 1Y Y+

Within Past 7 days 8 to 30 days ago 31 to 90 days ago 91 to 365 days ago

Known Exploitation: Mar 31, 2025 - Mar 30, 2026

Empirical Score 97.1% Top 1%

Score Distribution

Score History

Published Mar 24, 2025

Model Score Updated 5 days

Score Comparison

Local Test 97.1 (Top 1%)

Global 97.1 (Top 1%)

EPSS V4 23.0 (Top 4%)

See how your model would differ — book a walkthrough | empiralsecurity.com | info@empiralsecurity.com

EMPIRICAL

Foundation Features

The global model

01 Predictive scoring based on real exploitation likelihood	02 180,000+ CVEs covered, 18,000+ confirmed exploited	03 Near-real-time exploitation telemetry, updated hourly	04 Backed by a dedicated data science and research team	05 Full UI and API access
--	--	---	--	------------------------------

Radiant Features

The local model

Everything in Foundation, plus:	06 Custom model trained on your telemetry, assets, configurations, and vuln data	07 Continuously retrained to reflect changes in your environment	08 Full data isolation, only you access your model
---------------------------------	---	---	---

We bring measurable impact

Past solutions can’t prioritize, assess, and handle effective inference at scale. With Empirical, our models provide understanding and superior prioritization.

18,000+

Known Exploited Vulns
(and hourly telemetry about when exploitation occurred)

12.4x

A 1249.04% increase in total exploited CVEs as of January 9th, 2025 compared to CISA Known Exploited Vulnerabilities (KEV)

23x

4925 newly exploited CVEs in the last 12 months, compared to 204 in CISA KEV

