



Global Models

Global models combine real-time internet exploitation telemetry with EPSS predictions to provide the most accurate view of exploitation. It monitors activity over 16,000 known exploited in the wild CVEs, and uses that data in the model. This is 12x DHS CISA's KEV, and far more than any other vendor out there.

Our Global 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.

API

Search...

Models

Performance Explore Thresholds

Known Exploitation Activity

Empirical combines real-time internet exploitation telemetry with EPSS predictions to provide the most accurate view of exploitation.

New Activity

13

Known Exploitation Activity

1 Week ago

6,249

Known Exploitation Activity

1 Month ago

7,741

Known Exploitation Activity

3 Months ago

10,210

Known Exploitation Activity

1 Year ago

11,664

Known Exploitation Activity

Over a Year ago

15,319

Known Exploitation Activity

Empirical outputs a probability (0%–100%) of exploitation activity being observed in the next 30 days. Because it's a continuous value, the "point" slides across the plot, creating a line from high efficiency to high coverage.

EPSS v4 Model (30 days ago)

Global Model (30 days ago)

Global Vulns Distribution by Empirical Score

Our global model leverages datasets we buy, curate, and data mine with machine learning to build sophisticated solutions that are constantly updated and refined.

Empirical Security

app.empiricalsecurity.com/search?page=6&q=exploitation_activity%3A0-7&sort_by=score&sort_dir=asc

EMPIRICAL GLOBAL Data Models API Search... Settings Log Out

exploitation_activity:0-7

New Activity
12
Known Exploitation Activity

1 Week ago
6,827
Known Exploitation Activity

1 Month ago
6,574
Known Exploitation Activity

3 Months ago
6,713
Known Exploitation Activity

1 Year ago
6,671
Known Exploitation Activity

Over a Year ago
6,270
Known Exploitation Activity

1 Query

6,827 Results

Actions

6 of 342

SHARED

All Vulns

Threshold Beta – score:
[66.37 97.14]

Redhat

PRIVATE

Empirical Score

CVE ID

94.0% Top 3% CVE-2021-27165

94.1% Top 3% CVE-2004-1154

94.1% Top 3% CVE-2015-0048

94.1% Top 3% CVE-2021-27173

94.2% Top 3% CVE-2021-27170

94.3% Top 3% CVE-2014-6363

94.4% Top 3% CVE-2013-0019

94.4% Top 3% CVE-2010-2099

94.4% Top 3% CVE-2021-22779

94.4% Top 3% CVE-2024-27173

94.4% Top 3% CVE-2015-2321

94.4% Top 3% CVE-2015-1375

94.4% Top 3% CVE-2021-35298

94.4% Top 3% CVE-2023-28206

94.5% Top 3% CVE-2018-12519

94.5% Top 3% CVE-2015-8523

94.6% Top 3% CVE-2017-17664

94.7% Top 3% CVE-2015-3422

94.7% Top 3% CVE-2012-2614

94.7% Top 3% CVE-2021-27177

CVE-2023-28206

Details Exploit Code Chatter Malware

Summary

An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in macOS Monterey 12.6.5, iOS 16.4.1 and iPadOS 16.4.1, macOS Ventura 13.3.1, iOS 15.7.5 and iPadOS 15.7.5, macOS Big Sur 11.7.6. An app may be able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited.

Tags

Execute arbitrary code with kernel privileges, out of bounds memory write, code execution, input validation, out-of-bounds write

Known Exploitation Activity

Last Known: Jul 29, 2025 4 Known Sources Within Past 7 days

91 to 365 days ago Over 1 year ago

Vendors and Products

apple ipados iphone_os macos

Empirical Score

94.4% Top 3%

Score History

100% 10% 1% 0%

Mar 15, 2025 – May 31, 2025

Published

2023-04-10

Model Score Updated

3 days ago

Score Comparison

100% 50% 0%

0.3% 23.3% 94.4%

EPSS V3 EPSS V4 Global

CVSS

CVSS v3.1

8.6

Vector

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

Sources

134c704f-9b21-4f2e-91b3-4a467353bcc0, nvd@nist.gov

Compare Model Features

<div>ALL MODELS</div> <div><input type="checkbox"/> EPSS<input type="checkbox"/> GLOBAL<input type="checkbox"/> LOCAL</div> <div>Predictive Vulnerability Scoring</div>	<div>ALL MODELS</div> <div><input type="checkbox"/> EPSS<input type="checkbox"/> GLOBAL<input type="checkbox"/> LOCAL</div> <div>Hourly Score Updates and Enterprise Support</div>	<div>ALL MODELS</div> <div><input type="checkbox"/> EPSS<input type="checkbox"/> GLOBAL<input type="checkbox"/> LOCAL</div> <div>Legacy Model Support (EPSS v3, v4)</div>	<div>ALL MODELS</div> <div><input type="checkbox"/> EPSS<input type="checkbox"/> GLOBAL<input type="checkbox"/> LOCAL</div> <div>UI and API for Data Discovery & Model Performance</div>
<div>GLOBAL + LOCAL MODELS</div> <div><input checked="" type="checkbox"/> EPSS<input type="checkbox"/> GLOBAL<input type="checkbox"/> LOCAL</div> <div>Data on over 16,000 exploited in the wild CVEs</div>	<div>GLOBAL + LOCAL MODELS</div> <div><input checked="" type="checkbox"/> EPSS<input type="checkbox"/> GLOBAL<input type="checkbox"/> LOCAL</div> <div>Near-Real Time Exploitation Telemetry & Model</div>	<div>GLOBAL + LOCAL MODELS</div> <div><input checked="" type="checkbox"/> EPSS<input type="checkbox"/> GLOBAL<input type="checkbox"/> LOCAL</div> <div>ML model for discovering new exploit code on GitHub</div>	<div>GLOBAL + LOCAL MODELS</div> <div><input checked="" type="checkbox"/> EPSS<input type="checkbox"/> GLOBAL<input type="checkbox"/> LOCAL</div> <div>All Underlying data contributing to the model exposed</div>
<div>LOCAL MODELS</div> <div><input checked="" type="checkbox"/> EPSS<input checked="" type="checkbox"/> GLOBAL<input type="checkbox"/> LOCAL</div> <div>Custom Vulnerability Model based on your attack telemetry, asset data, vuln data, & threat intelligence</div>	<div>LOCAL MODELS</div> <div><input checked="" type="checkbox"/> EPSS<input checked="" type="checkbox"/> GLOBAL<input type="checkbox"/> LOCAL</div> <div>Model Performance Measured against your attack telemetry</div>	<div>LOCAL MODELS</div> <div><input checked="" type="checkbox"/> EPSS<input checked="" type="checkbox"/> GLOBAL<input type="checkbox"/> LOCAL</div> <div>Forward Deployed Data Science Team</div>	<div>LOCAL MODELS</div> <div><input checked="" type="checkbox"/> EPSS<input checked="" type="checkbox"/> GLOBAL<input type="checkbox"/> LOCAL</div> <div>Only you will have access to your model</div>

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.

6x

More efficient than CVSS (comparison vs. EPSS, our free model, at 87% coverage)

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

