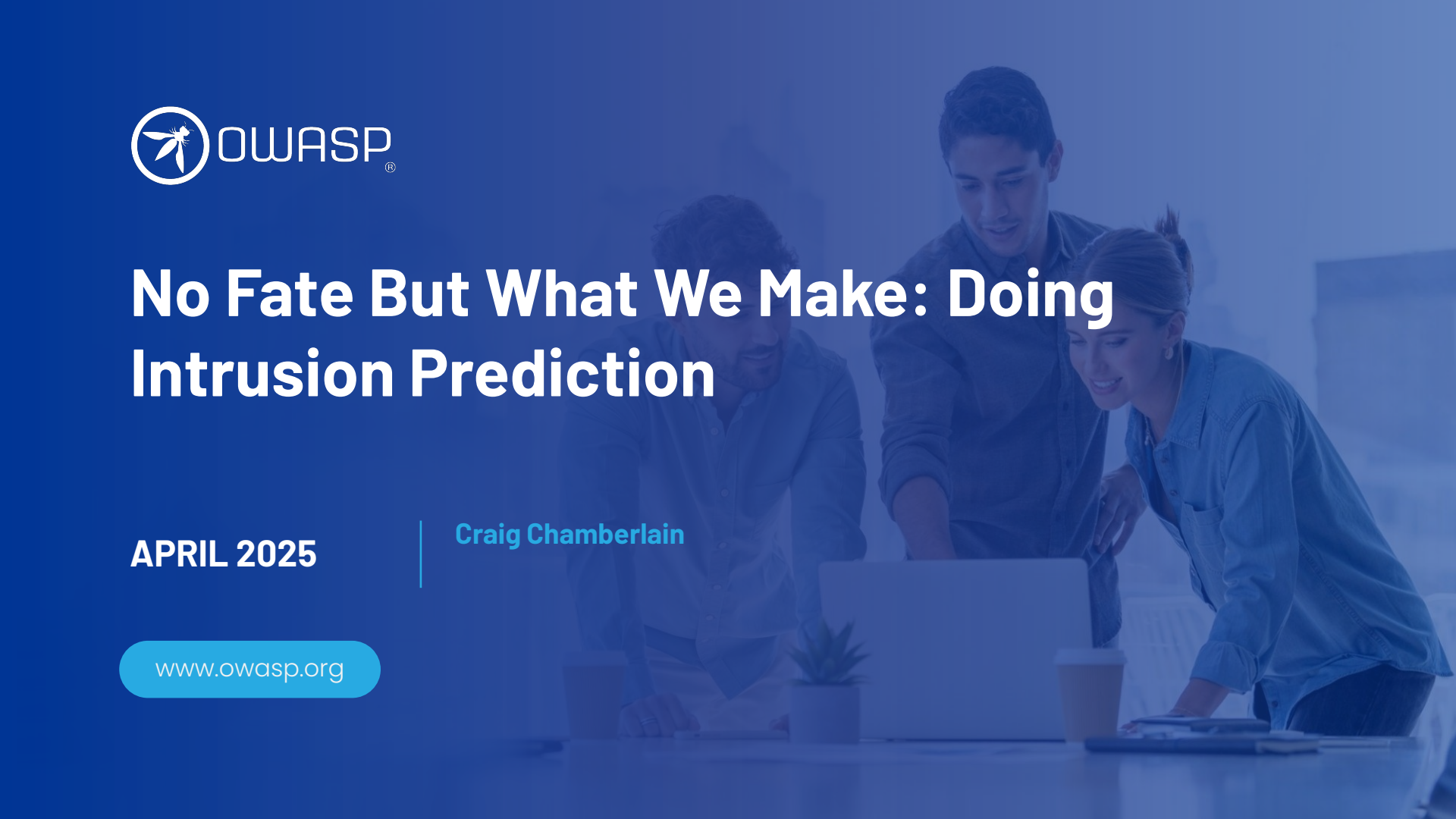


No Fate But What We Make: Doing Intrusion Prediction

APRIL 2025

Craig Chamberlain

www.owasp.org

Founder, OpenDR

Craig Chamberlain

Craig Chamberlain has been working on threat hunting and detection for most of his life. He has contributed to several products you may have used. He has been a principal at six startups, four of which had successful exits, and including four security products. He has presented at numerous conferences including the SANS Threat Hunting Summit; CactusCon; the ISC2 Congress; RSA; DEF CON; SOURCE Boston; and several B-Sides conferences.

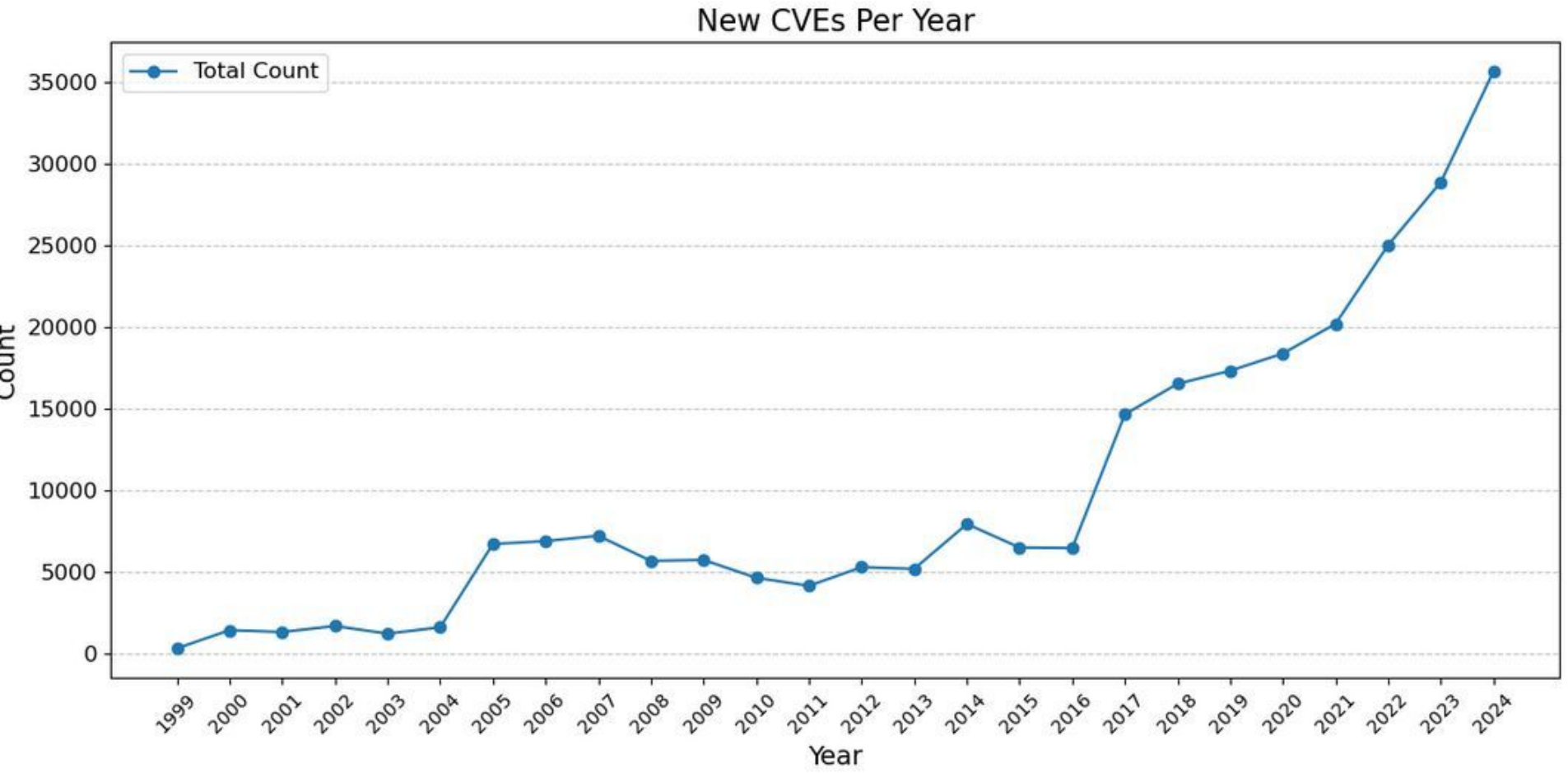
INTRODUCTION

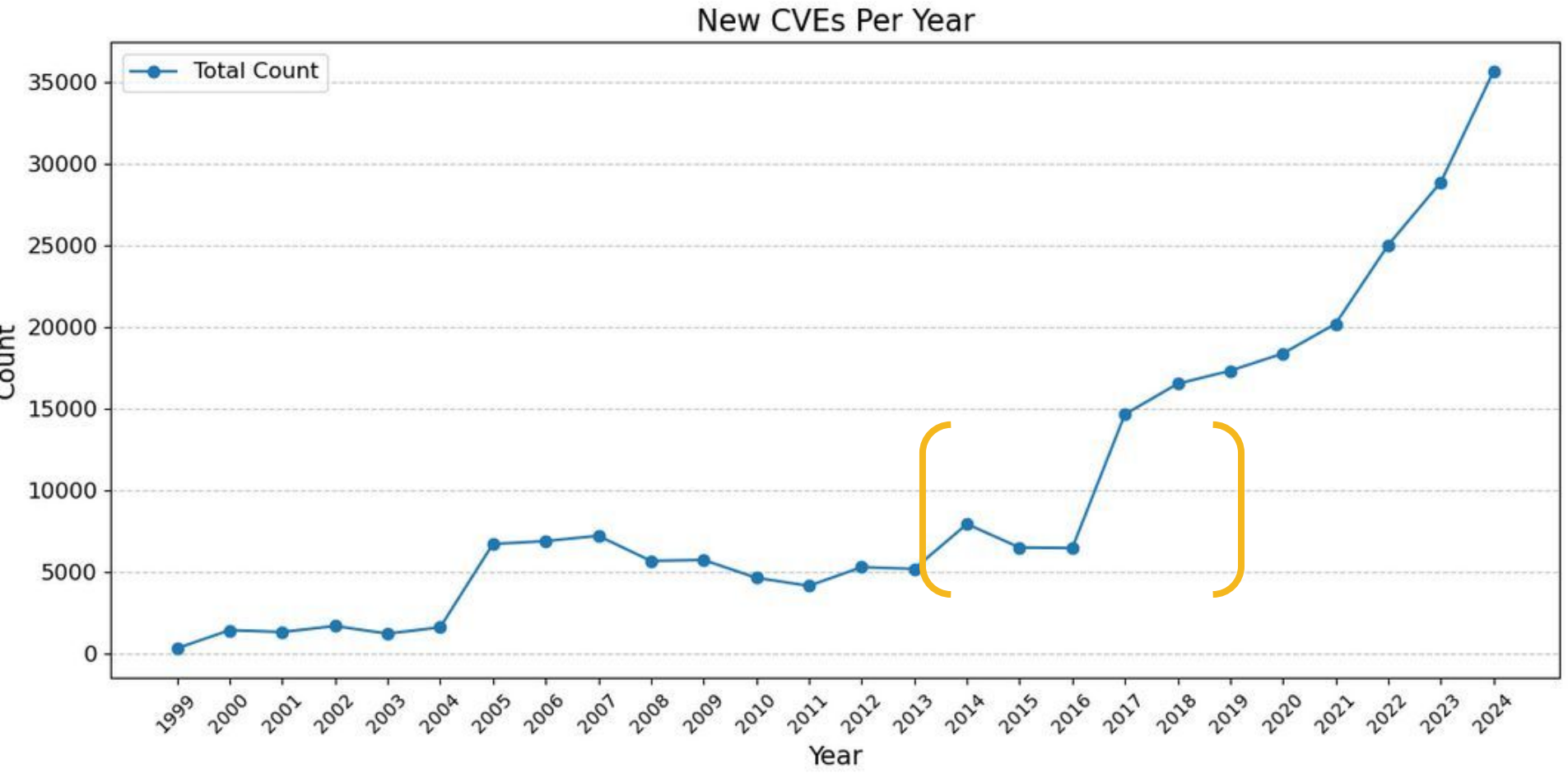
INTRODUCTION

CVE, CVSS, EPSS, exploit-ability, reach-ability, risk based scoring, AI, lol..we use a bewildering and growing number of complex methods in an attempt to identify which CVEs are the ones that present the greatest technical or business risk. CVE volume increases year by year and some of our methodologies were developed in prior decades, when CVE volume was a fraction of what is is today. We can't predict which CVEs are going to go 'hot' in the future - but what if we could? This is the story of the NOFATE project, which is part of the SKYNET project for eliminating alert fatigue at scale.NOFATE has, since Jan. 3, published 25 correct predictions on CVEs being added to a KEV watchlist, with early warning times as long as 30 - 90 days. If we can predictively micro-target the few 'superhot' CVEs for action quickly, around the same time they are released, we could be doing intrusion prediction, and incident avoidance, rather than doing threat detection and incident response in a series of CVE and incident fire drills. The predictions are published on GitHub.

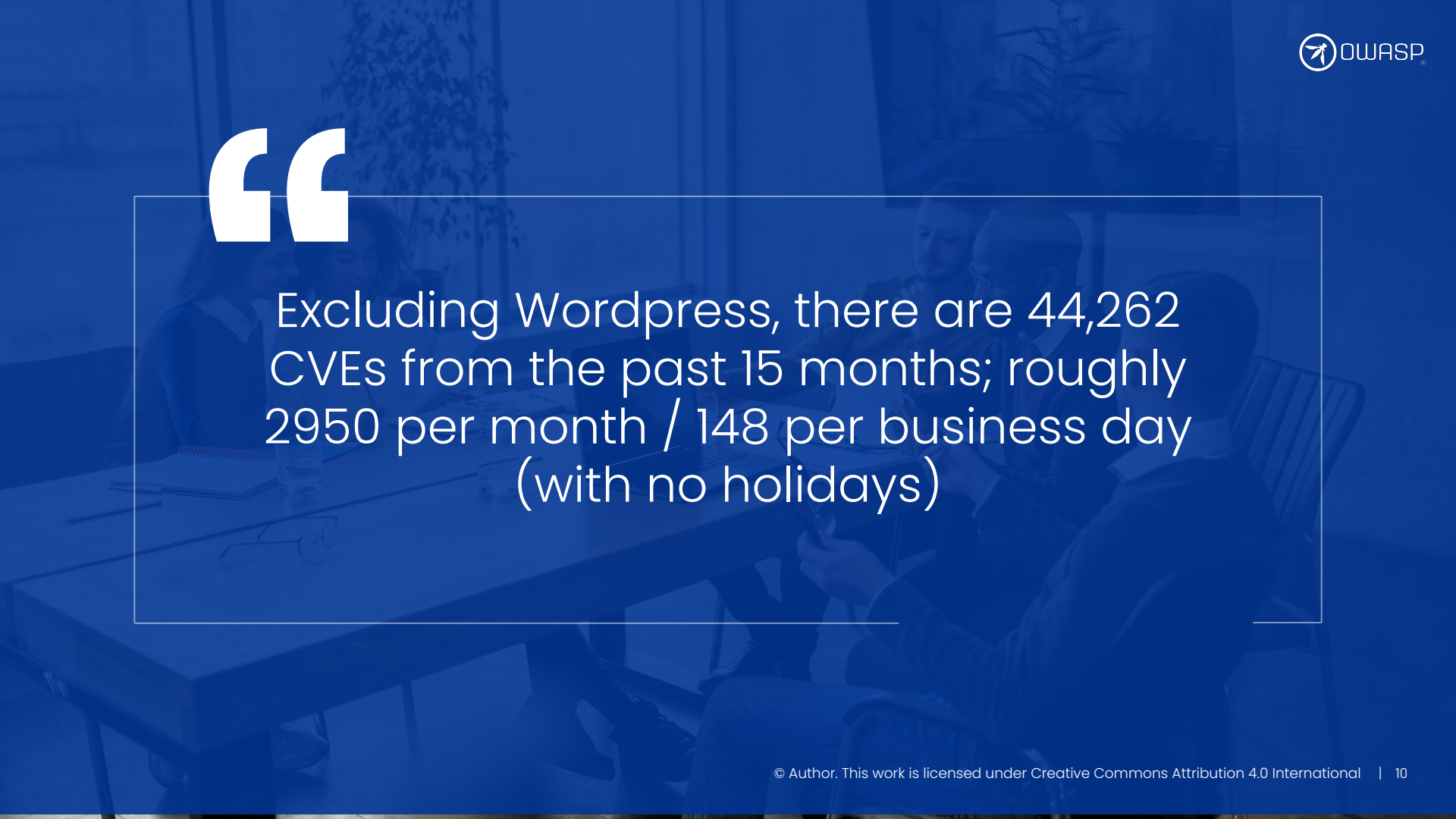
This is the story of why I created a model that has generated 25 correct CVE predictions forward in time with early warning times as long as 93 days.

274,000


New CVEs Per Year
Total Count
35000
30000
25000
20000
15000
10000
5000
0
Count
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
Year

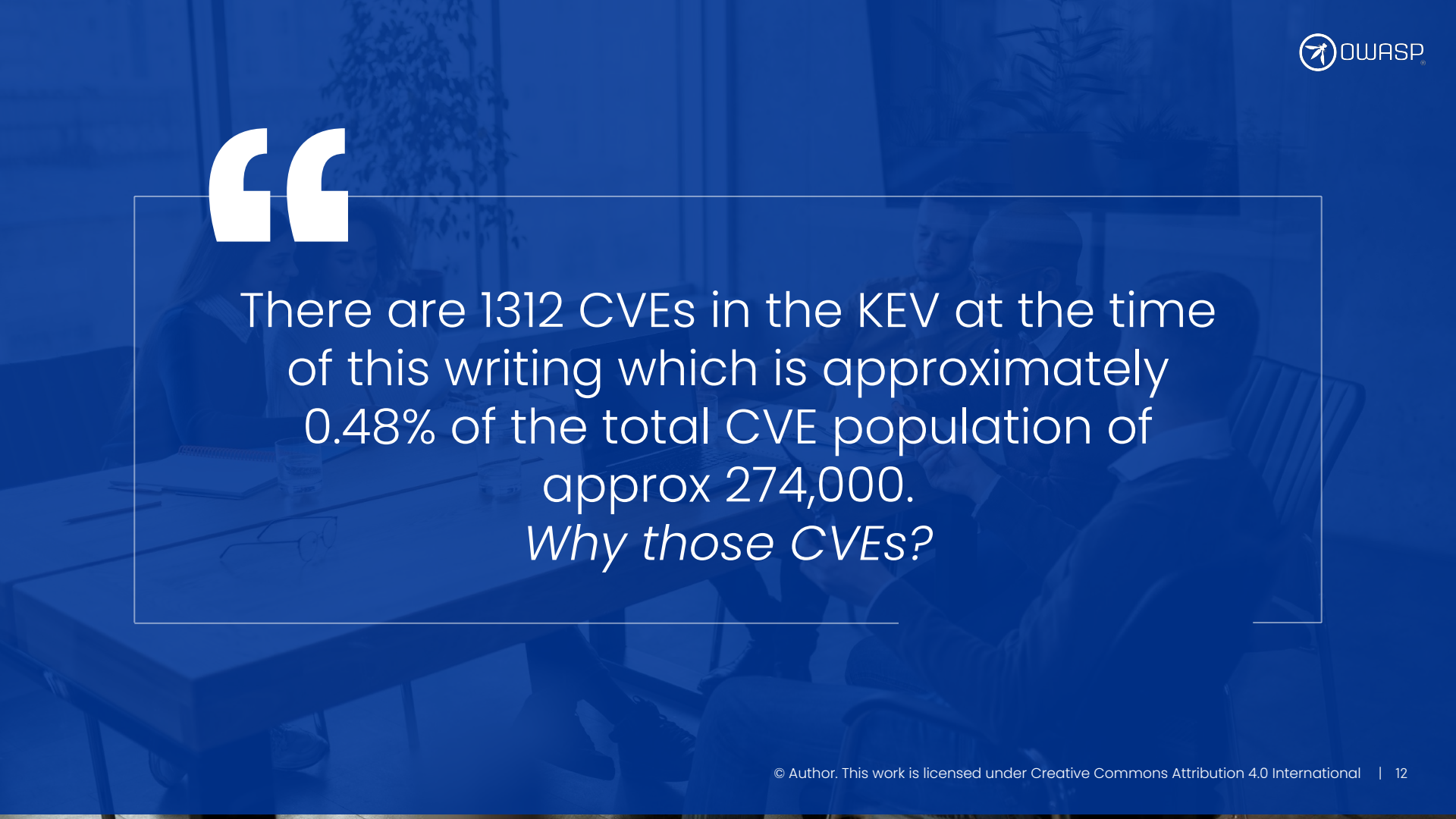

New CVEs Per Year
Total Count
35000
30000
25000
20000
15000
10000
5000
0
Count
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
Year

2950
148



> Excluding Wordpress, there are 44,262 CVEs from the past 15 months; roughly 2950 per month / 148 per business day (with no holidays)

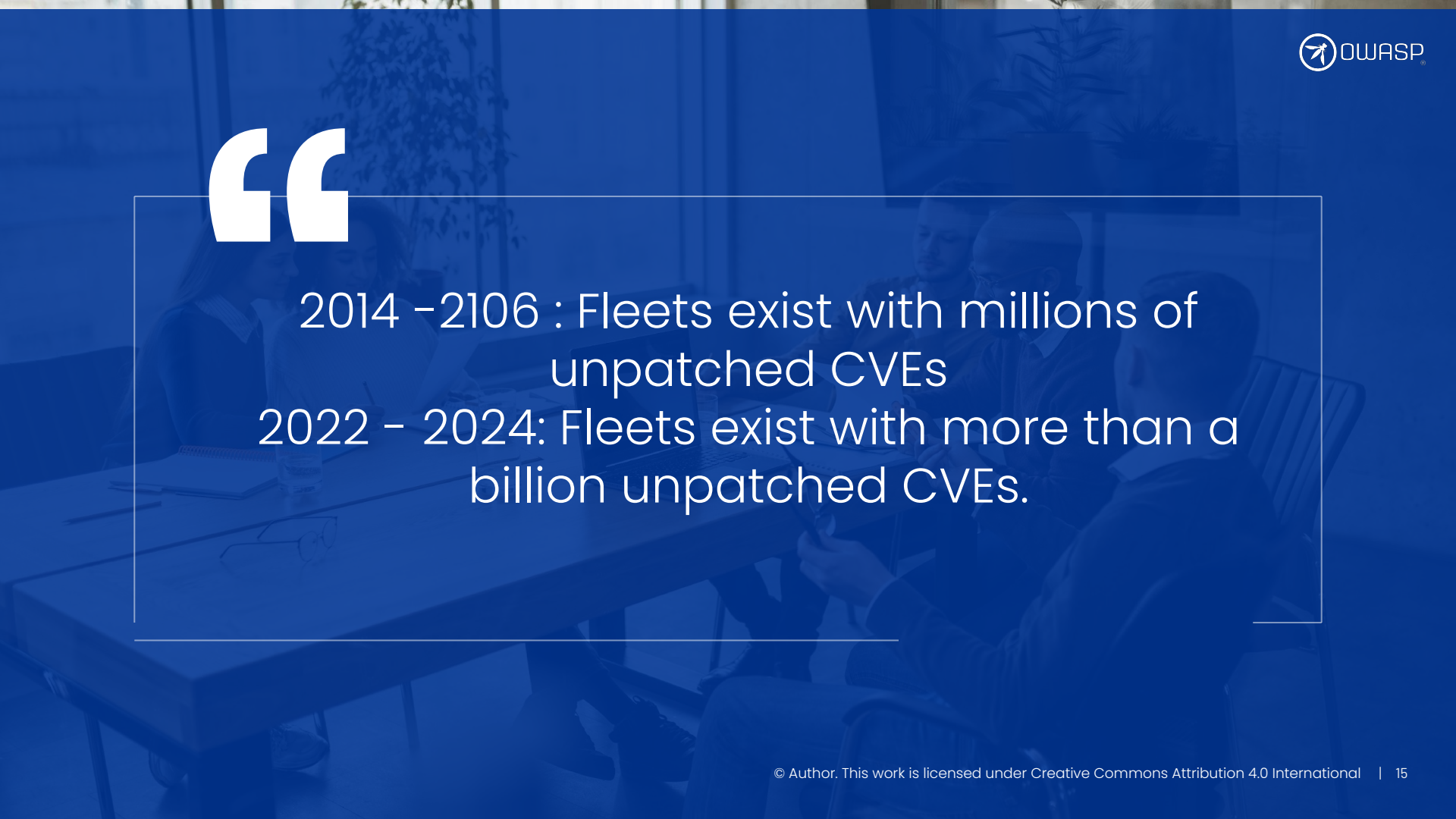
1312



There are 1312 CVEs in the KEV at the time of this writing which is approximately 0.48% of the total CVE population of approx 274,000.
Why those CVEs?

> Offensive actors - threats and red teams - are choosing exploits more than CVEs, which relates to a CVE choice, but they're not looking at them the same way we do.

2014 - 2016 : “We’re not going to 100% patch convergence, with the resources we have, so how should we manage this? How can we determine which ones have the highest business risk?”



2014 -2106 : Fleets exist with millions of unpatched CVEs
2022 - 2024: Fleets exist with more than a billion unpatched CVEs.

LET'S DO SOME DATA

(IN A NOTEBOOK)

https://github.com/cyberdyne-ventures/predictions

25 Predictions

A repo for publishing the output of an experimental intrusion prediction project. Output is posted here where it is time stamped so that any correct predictions can be verified in linear time without creating a causality loop. A rating of 'hot' means the CVE will land on one or more watchlists due to significance, exploitation and / or impact.

This project has its own license.

Provable predictions so far (total 25) - provable meanining the prediction was publshed here some time - days or months - before the CVE went 'hot' meaning it was added to a watchlist of widely exploited critical vulns.

March 31: CVE-2024-20439 was added to the KEV. It was was rated hot in the January 3 run which is the longest lead time yet at 94 days! `CVE-2024-20439 Cisco Cisco Smart License Utility "A vulnerability in Cisco Smart Licensing Utility could allow an unauthenticated, remote attacker to log in to an affected system by using a static administrative credential.`

March 18: CVE-2025-24472 was added to the KEV. It was rated hot in the Feb 15 run, another 31 day lead time. `CVE-2025-24472 Fortinet FortiOS "An Authentication Bypass Using an Alternate Path or Channel vulnerability [CWE-288] affecting FortiOS 7.0.0 through 7.0.16 and FortiProxy 7.2.0 through 7.2.12, 7.0.0 through 7.0.19 may allow a remote attacker to gain super-admin privileges via crafted CSF proxy requests." hot`

March 10: CVE-2025-25151 was added to the KEV. It was rated hot in the Feb 15 run. (23)

`CVE-2025-25181 Advantive VeraCore A SQL injection vulnerability in timeoutWarning.asp in Advantive VeraCore through 2025.1.0 allows remote attackers to execute arbitrary SQL commands via the PmSess1 parameter. hot`

March 10: CVE-2024-13159 was added to the KEV. It was rated hot in the Jan 17 run.

`CVE-2024-13159 hot Ivanti Endpoint Manager Absolute path traversal in Ivanti EPM before the 2024 January-2025 Security Update and 2022 SU6 January-2025 Security Update allows a remote unauthenticated attacker to leak sensitive information.`

March 10: CVE-2024-13160 was added to the KEV. It was rated hot in the Jan 17 run.

`CVE-2024-13160 hot Ivanti Endpoint Manager Absolute path traversal in Ivanti EPM before the 2024 January-2025 Security Update and 2022 SU6 January-2025 Security Update allows a remote unauthenticated attacker to leak sensitive information.`

> Intrusion prediction allows for incident avoidance as an alternative to incident response. With early warning times as long as 30-90 days, it will become possible to avoid exploitation.

> As offensive art is scaled and accelerated by large language models. We won't be able to move existing IR process fast enough to avoid exploitation cycles as they contract from days to hours. We need to think about avoidance vs. response.

Q&A

https://github.com/cyberdyne-ventures/predictions

25 Predictions

A repo for publishing the output of an experimental intrusion prediction project. Output is posted here where it is time stamped so that any correct predictions can be verified in linear time without creating a causality loop. A rating of 'hot' means the CVE will land on one or more watchlists due to significance, exploitation and / or impact.

This project has its own license.

Provable predictions so far (total 25) - provable meanining the prediction was publshed here some time - days or months - before the CVE went 'hot' meaning it was added to a watchlist of widely exploited critical vulns.

March 31: CVE-2024-20439 was added to the KEV. It was was rated hot in the January 3 run which is the longest lead time yet at 94 days! `CVE-2024-20439 Cisco Cisco Smart License Utility "A vulnerability in Cisco Smart Licensing Utility could allow an unauthenticated, remote attacker to log in to an affected system by using a static administrative credential.`

March 18: CVE-2025-24472 was added to the KEV. It was rated hot in the Feb 15 run, another 31 day lead time. `CVE-2025-24472 Fortinet FortiOS "An Authentication Bypass Using an Alternate Path or Channel vulnerability [CWE-288] affecting FortiOS 7.0.0 through 7.0.16 and FortiProxy 7.2.0 through 7.2.12, 7.0.0 through 7.0.19 may allow a remote attacker to gain super-admin privileges via crafted CSF proxy requests." hot`

March 10: CVE-2025-25151 was added to the KEV. It was rated hot in the Feb 15 run. (23)

`CVE-2025-25181 Advantive VeraCore A SQL injection vulnerability in timeoutWarning.asp in Advantive VeraCore through 2025.1.0 allows remote attackers to execute arbitrary SQL commands via the PmSess1 parameter. hot`

March 10: CVE-2024-13159 was added to the KEV. It was rated hot in the Jan 17 run.

`CVE-2024-13159 hot Ivanti Endpoint Manager Absolute path traversal in Ivanti EPM before the 2024 January-2025 Security Update and 2022 SU6 January-2025 Security Update allows a remote unauthenticated attacker to leak sensitive information.`

March 10: CVE-2024-13160 was added to the KEV. It was rated hot in the Jan 17 run.

`CVE-2024-13160 hot Ivanti Endpoint Manager Absolute path traversal in Ivanti EPM before the 2024 January-2025 Security Update and 2022 SU6 January-2025 Security Update allows a remote unauthenticated attacker to leak sensitive information.`

THANK YOU

FOR YOUR ATTENTION

ADDRESS

401 Edgewater Place, Suite 600
Wakefield, MA 01880

PHONE

+1 951-692-7703

E-MAIL

contact@owasp.org