DARPA + ARPA-H

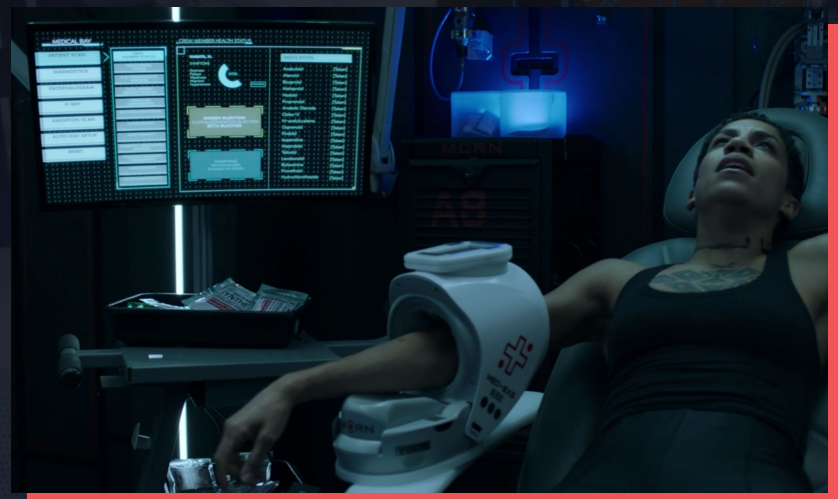
AIxCC
AI CYBER CHALLENGE

PATCHING CRITICAL INFRASTRUCTURE

Announcing the Winners of DARPA's AI Cyber Challenge

Andrew Carney

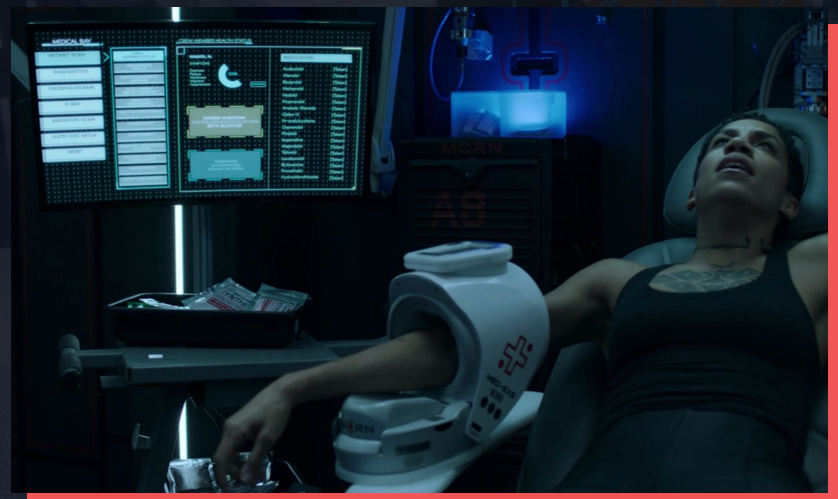
Replicator, “Star Trek”



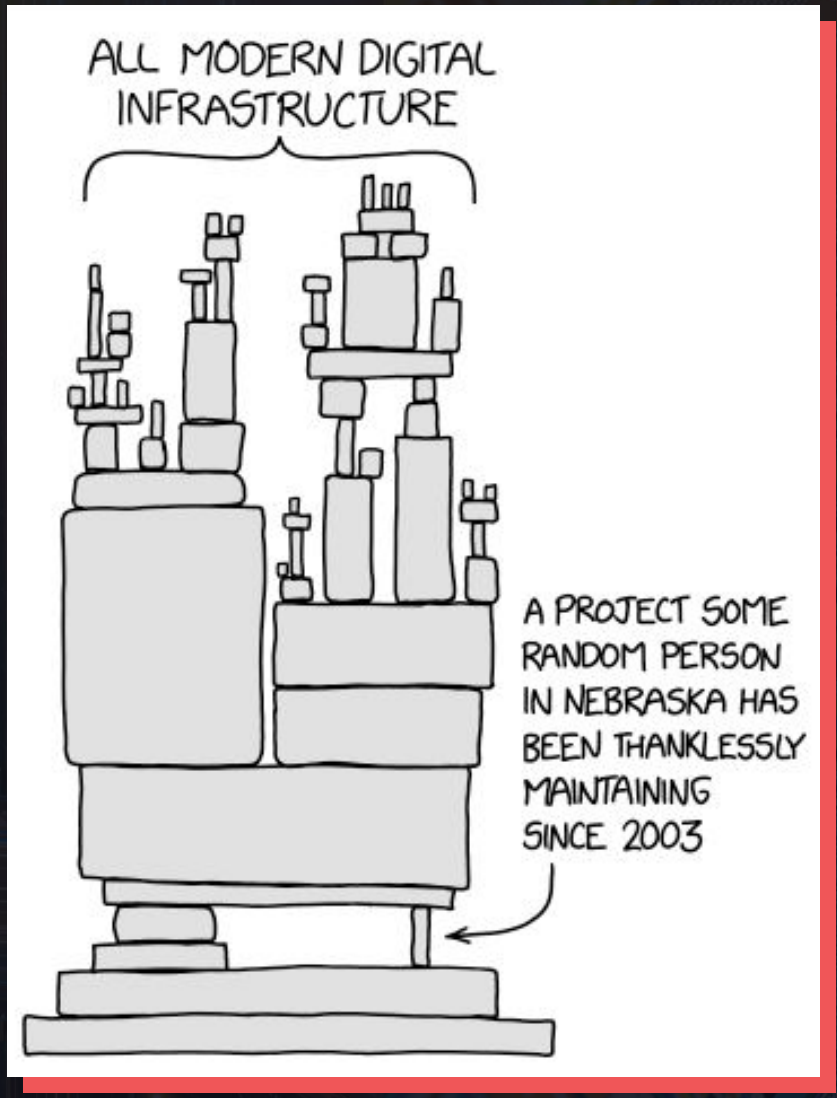
Autodoc, “The Expanse”

> ***Any sufficiently advanced technology is indistinguishable from magic.***
>
> - Arthur C. Clarke

Replicator, “Star Trek”



Autodoc, “The Expanse”



Unsophisticated Cyber Actor(s) Targeting Operational Technology

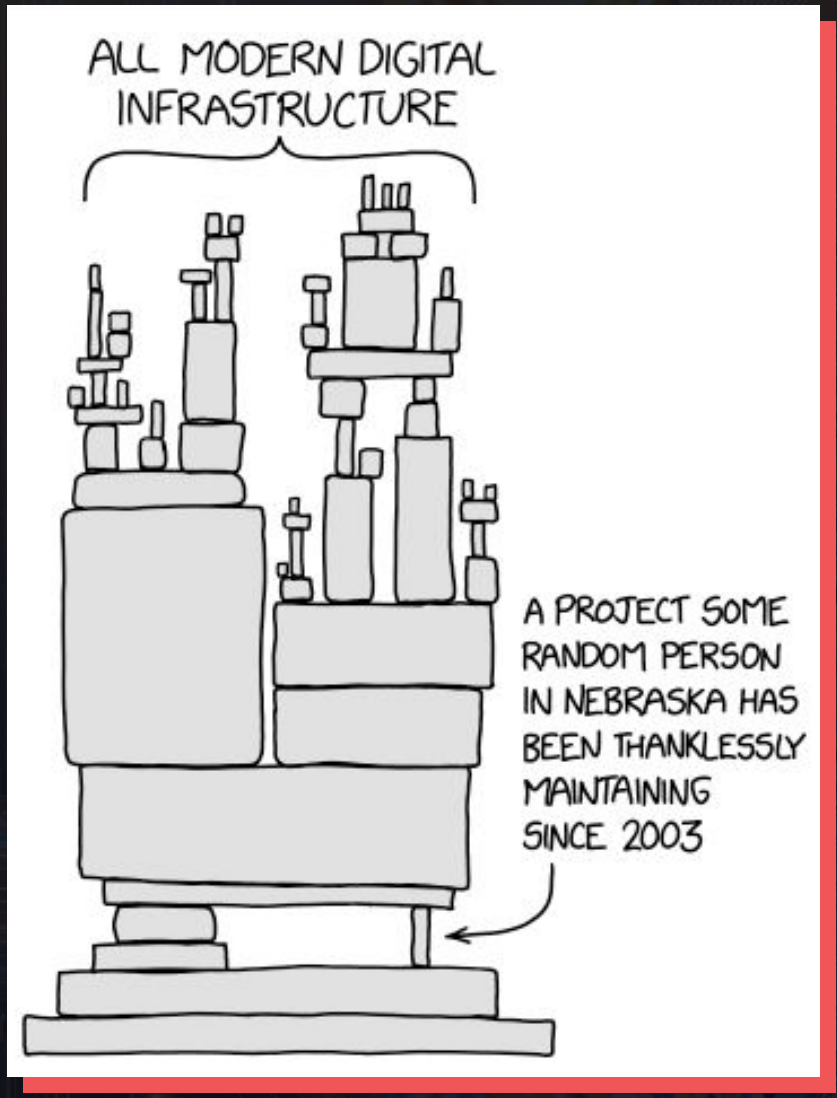
Release Date: May 06, 2025

Replicator, “Star Trek”

Autodoc, “The Expanse”

Critical infrastructure vulnerabilities

are incompatible with the future

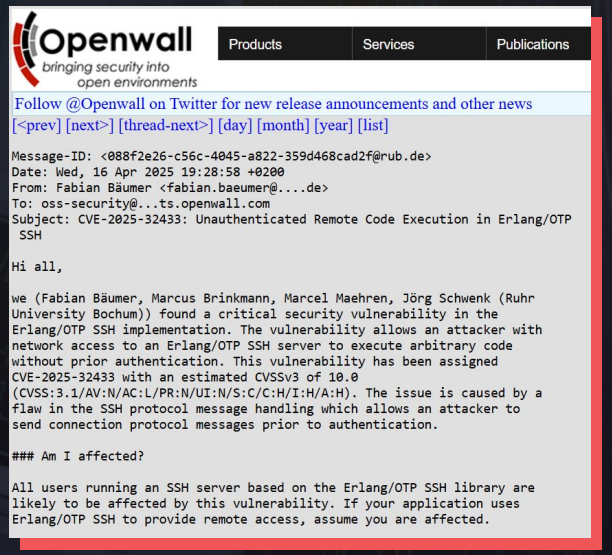


Unsophisticated Cyber Actor(s) Targeting Operational Technology

Release Date: May 06, 2025

OUR CRITICAL INFRASTRUCTURE DEPENDS ON OPEN SOURCE SOFTWARE AND IS VULNERABLE

We cannot move forward if critical vulnerabilities can survive in our code for years


Openwall
bringing security into open environments
Products Services Publications

Follow @Openwall on Twitter for new release announcements and other news
[<prev] [next>] [thread-next>] [day] [month] [year] [list]

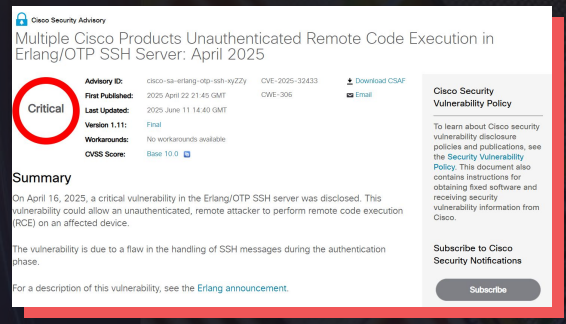
Message-ID: <088f2e26-c56c-4045-a822-359d468cad2f@rub.de>
Date: Wed, 16 Apr 2025 19:28:58 +0200
From: Fabian Bäumer <fabian.baeumer@....de>
To: oss-security@...ts.openwall.com
Subject: CVE-2025-32433: Unauthenticated Remote Code Execution in Erlang/OTP SSH

Hi all,

we (Fabian Bäumer, Marcus Brinkmann, Marcel Maehren, Jörg Schwenk (Ruhr University Bochum)) found a critical security vulnerability in the Erlang/OTP SSH implementation. The vulnerability allows an attacker with network access to an Erlang/OTP SSH server to execute arbitrary code without prior authentication. This vulnerability has been assigned CVE-2025-32433 with an estimated CVSSv3 of 10.0 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H). The issue is caused by a flaw in the SSH protocol message handling which allows an attacker to send connection protocol messages prior to authentication.

Am I affected?

All users running an SSH server based on the Erlang/OTP SSH library are likely to be affected by this vulnerability. If your application uses Erlang/OTP SSH to provide remote access, assume you are affected.


Cisco Security Advisory

Multiple Cisco Products Unauthenticated Remote Code Execution in Erlang/OTP SSH Server: April 2025

Critical

Advisory ID: cisco-sa-erlang-otp-ssh-xyZZy CVE-2025-32433 Download CSAF
First Published: 2025 April 22 21:45 GMT CWE-306 Email
Last Updated: 2025 June 11 14:40 GMT
Version 1.11: Final
Workarounds: No workarounds available
CVSS Score: Base 10.0

Summary

On April 16, 2025, a critical vulnerability in the Erlang/OTP SSH server was disclosed. This vulnerability could allow an unauthenticated, remote attacker to perform remote code execution (RCE) on an affected device.

The vulnerability is due to a flaw in the handling of SSH messages during the authentication phase.

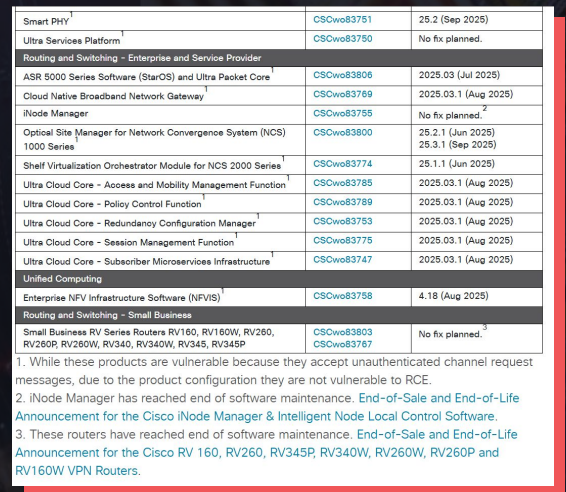
For a description of this vulnerability, see the Erlang announcement.

Cisco Security Vulnerability Policy

To learn about Cisco security vulnerability disclosure policies and publications, see the Security Vulnerability Policy. This document also contains instructions for obtaining fixed software and receiving security vulnerability information from Cisco.

Subscribe to Cisco Security Notifications

Subscribe



Smart PHY[1]	CSCwo83751	25.2 (Sep 2025)
Ultra Services Platform[1]	CSCwo83750	No fix planned.
Routing and Switching - Enterprise and Service Provider		
ASR 5000 Series Software (StarOS) and Ultra Packet Core[1]	CSCwo83806	2025.03 (Jul 2025)
Cloud Native Broadband Network Gateway[1]	CSCwo83769	2025.03.1 (Aug 2025)
iNode Manager	CSCwo83755	No fix planned.[2]
Optical Site Manager for Network Convergence System (NCS) 1000 Series[1]	CSCwo83800	25.2.1 (Jun 2025) 25.3.1 (Sep 2025)
Shelf Virtualization Orchestrator Module for NCS 2000 Series[1]	CSCwo83774	25.1.1 (Jun 2025)
Ultra Cloud Core - Access and Mobility Management Function[1]	CSCwo83785	2025.03.1 (Aug 2025)
Ultra Cloud Core - Policy Control Function[1]	CSCwo83789	2025.03.1 (Aug 2025)
Ultra Cloud Core - Redundancy Configuration Manager[1]	CSCwo83753	2025.03.1 (Aug 2025)
Ultra Cloud Core - Session Management Function[1]	CSCwo83775	2025.03.1 (Aug 2025)
Ultra Cloud Core - Subscriber Microservices Infrastructure[1]	CSCwo83747	2025.03.1 (Aug 2025)
Unified Computing		
Enterprise NFV Infrastructure Software (NFVIS)[1]	CSCwo83758	4.18 (Aug 2025)
Routing and Switching - Small Business		
Small Business RV Series Routers RV160, RV160W, RV260, RV260P, RV260W, RV340, RV340W, RV345, RV345P	CSCwo83803 CSCwo83767	No fix planned.[3]

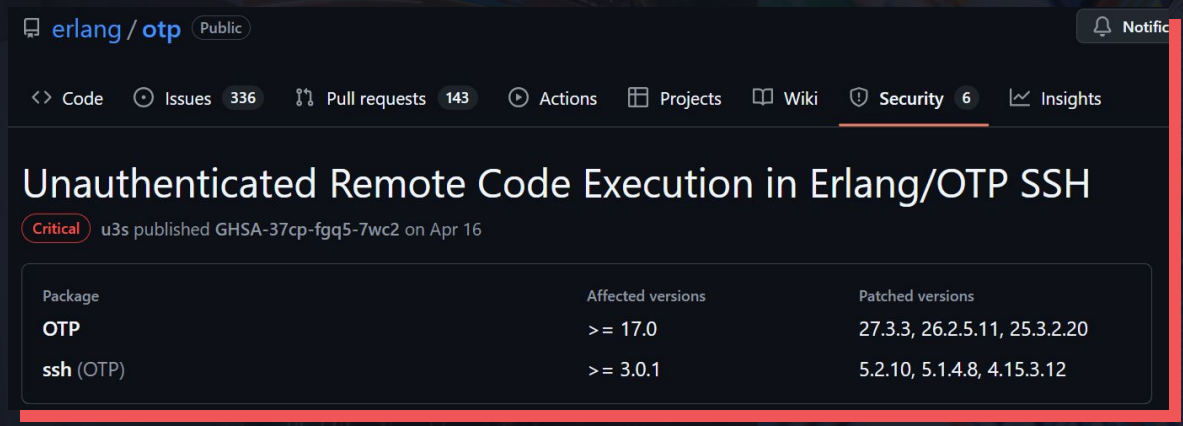
1. While these products are vulnerable because they accept unauthenticated channel request messages, due to the product configuration they are not vulnerable to RCE.
2. iNode Manager has reached end of software maintenance. End-of-Sale and End-of-Life Announcement for the Cisco iNode Manager & Intelligent Node Local Control Software.
3. These routers have reached end of software maintenance. End-of-Sale and End-of-Life Announcement for the Cisco RV 160, RV260, RV345P, RV340W, RV260W, RV260P and RV160W VPN Routers.


CISA Adds Two Known Exploited Vulnerabilities to Catalog

Release Date: June 09, 2025

CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation.

- CVE-2025-32433 Erlang Erlang/OTP SSH Server Missing Authentication for Critical Function Vulnerability
- CVE-2024-42009 RoundCube Webmail Cross-Site Scripting Vulnerability


erlang / otp Public Notific

Code Issues 336 Pull requests 143 Actions Projects Wiki Security 6 Insights

Unauthenticated Remote Code Execution in Erlang/OTP SSH

Critical u3s published GHSA-37cp-fgq5-7wc2 on Apr 16

Package	Affected versions	Patched versions
OTP	>= 17.0	27.3.3, 26.2.5.11, 25.3.2.20
ssh (OTP)	>= 3.0.1	5.2.10, 5.1.4.8, 4.15.3.12

AIxCC
AI CYBER CHALLENGE

DARPA + ARPA-H

AIxCC

AI CYBER CHALLENGE

DARPA + ARPA-H

AIxCC
AI CYBER CHALLENGE

WHAT IS AIxCC?

- A competition that rewards autonomous systems that find and patch vulnerabilities in source code.
- The challenges are well-known open-source projects.
- The vulnerabilities are realistic or real.
- Patching is worth more than finding.
- Code and data will be released open source.

Bug vs. vulnerability

Sometimes, magic is just someone spending more time on something than anyone else might reasonably expect.

- Teller (of Penn and Teller)

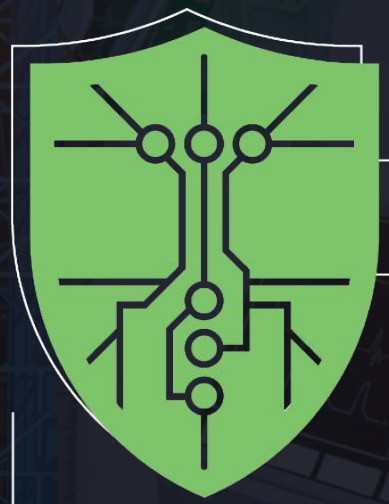
AIxCC
AI CYBER CHALLENGE

Bug vs. vulnerability

> ***Sometimes, [a vulnerability] is just someone spending more time on [a bug] than anyone else might reasonably expect.***
>
> - Teller (of Penn and Teller)

AIxCC
AI CYBER CHALLENGE

Preliminary events



Top 7 teams advance

black hat

AUGUST 2023

OPEN TRACK AND SMALL BUSINESS TRACK SUBMISSIONS

DEFCON

AUGUST 2024

SEMIFINAL COMPETITION

Top 7 teams $2 million each

DEFCON

AUGUST 2025

FINAL COMPETITION

Winners announced

1ST: $4 MILLION

2ND: $3 MILLION

3RD: $1.5 MILLION

Google ANTHROP\C OpenAI Microsoft THE LINUX FOUNDATION OpenSSF OPEN SOURCE SECURITY FOUNDATION

AIxCC
AI CYBER CHALLENGE

SEMIFINAL COMPETITION
OVERVIEW

DARPA + ARPA-H

To help secure our critical infrastructure, teams created custom CRSs that competed in the AIxCC Semifinal Competition.

42 TEAMS COMPETED

S9

synthetic vulnerabilities

7 TEAMS ADVANCE TO FINALS

5 CHALLENGE PROJECTS

- Linux Kernel
- NGINX
- Tika
- Jenkins
- SQLite

4 hours per round

an AI budget constraint of

$100 PER ROUND

each teams CRS had access to

3 nodes

each with

64 cores

256 GB RAM

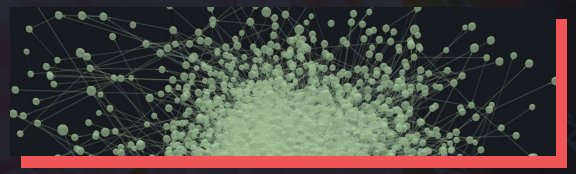
FINALS COMPETITION

COLLABORATORS & PARTNERS

Google ANTHROPIC OpenAI Microsoft THE LINUX FOUNDATION OpenSSF OPEN SOURCE SECURITY FOUNDATION blackhat DEFCON

NOTE: Teams in alphabetical order.

What counts for semifinals?



Proof-Of-Vulnerability (POV)

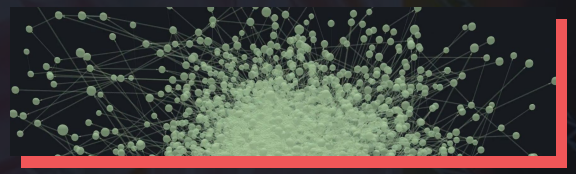
- Input data to reproduce vulnerability crash in harness

PATCH

- Unified diff source code fix for vulnerabilities

AIxCC
AI CYBER CHALLENGE

What counts for finals?

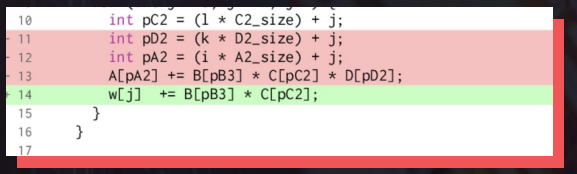


Proof-Of-Vulnerability (POV)

- Input data to reproduce vulnerability crash in harness

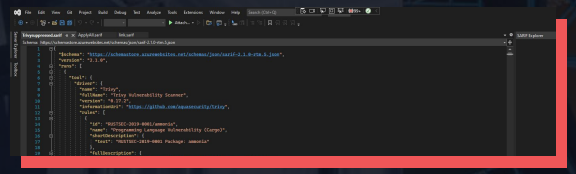
PATCH

- Unified diff source code fix for vulnerabilities



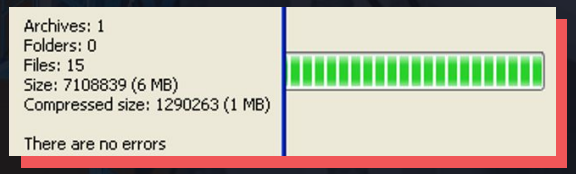
DELTA SCAN

- Challenge analyzing base code plus applied diff changes



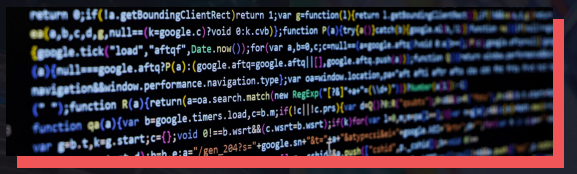
SARIF Assessment

- Structured reporting format for vulnerability details



BUNDLE

- Grouping of related PoV, patch, and SARIF submissions

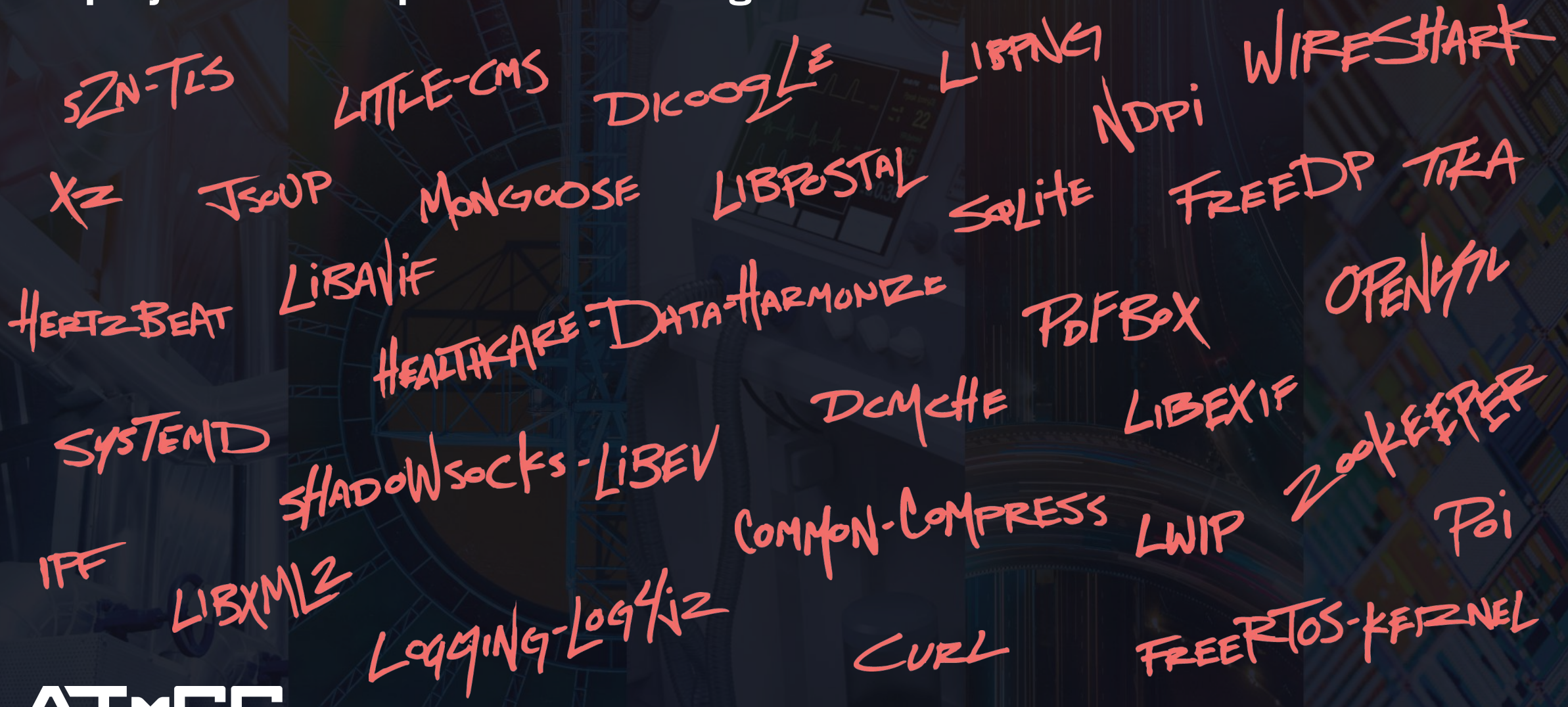


FULL SCAN

- Challenge analyzing entire code base

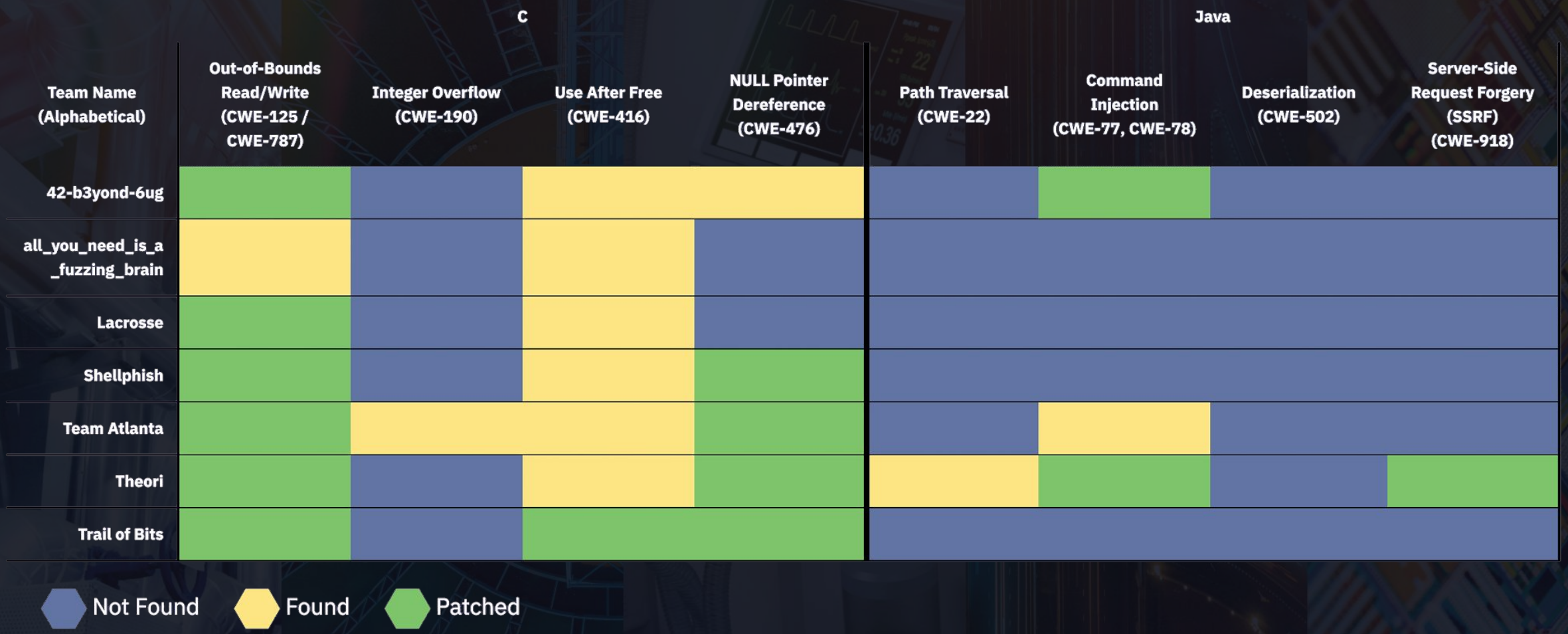
AIxCC
AI CYBER CHALLENGE

All projects we adapted into challenges

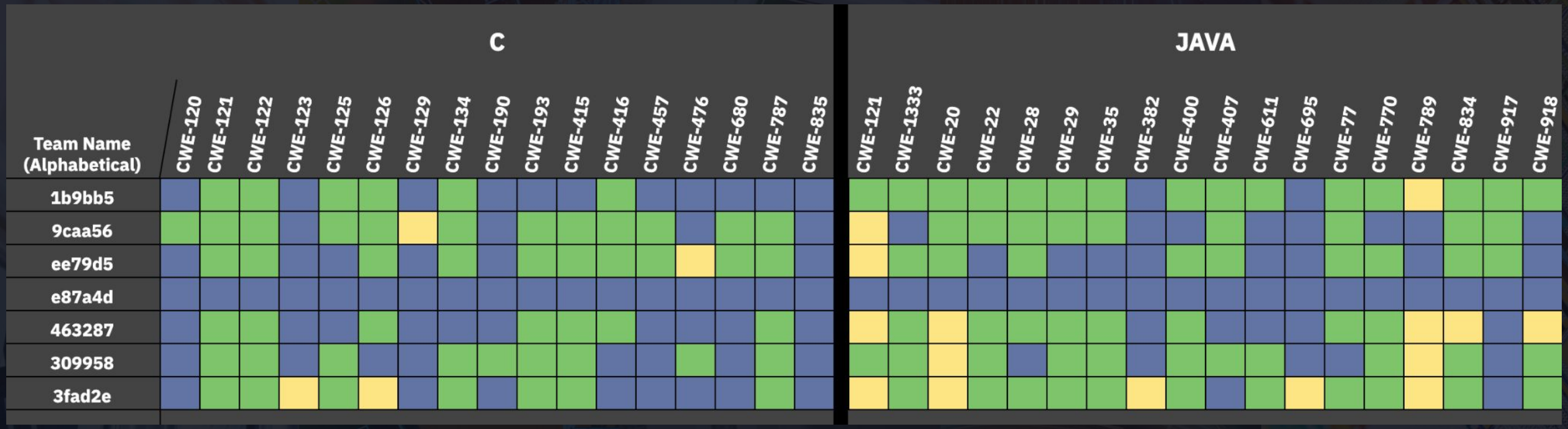


AIxCC
AI CYBER CHALLENGE

Semifinal Competition CRS performance by vulnerability class - synthetic only



Final Competition CRS performance by vulnerability class - synthetic only



Not Found Found Patched

COMPETITION AGGREGATE RESULTS - SYNTHETIC VULNERABILITIES

Semifinal
(5 Repositories / 59 Challenges)

Vulnerabilities discovered

37% (22/59)

Vulnerabilities patched

25% (15/59)

Avg. Time to patch

2 hours

Final
(28 Repositories / 53 Challenges)

Known Vulnerabilities discovered

77% (54/70)

Known Vulnerabilities patched

61% (43/70)

Avg. Time to patch

45 minutes

COMPETITION AGGREGATE RESULTS - REAL WORLD, NON-SYNTHETIC VULNERABILITIES

Semifinal

Found in C

1

Found in Java

0

Final

Found in C

6 (1 replay - SystemD)

Found in Java

12

Patched in C

0

Patched in Java

11 (3 w/o PoV)

* More information pending disclosure completion

FINAL ROUND DATA POINTS

Total Known Vulnerabilities
70

Real World Vulns discovered
18

Total spent (Compute + LLM)
$359k

Vulnerabilities discovered
54 (77%)

Average time to patch
45 min

Total LLM queries
1.9M

Vulnerabilities patched
43 (61%)

Total LOC analyzed
54M

LLM Spend
$82k

AIxCC
AI CYBER CHALLENGE

COST PER TASK SUCCESS
(PoV, Patch, SARIF, or a Bundle)

~$152

AIxCC
AI CYBER CHALLENGE


CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA

DEFCON


NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA


KUDU DYNAMICS
A Leidos Company


BLUESKY
INNOVATORS


UNDAUNTED


theDifference


NTIA


OSTIF
CELEBRATING 10 YEARS!


SPA
SYSTEMS PLANNING & ANALYSIS


OpenSSF
OPEN SOURCE SECURITY FOUNDATION


ANTHROPIC


DEPARTMENT OF TRANSPORTATION
UNITED STATES OF AMERICA


Dazzle Cat Duo


GAG LAB


RHAPSODE
CONSULTING


Google


DEPARTMENT OF ENERGY
UNITED STATES OF AMERICA


ses


Designated Defense
Security Services


CROMULENCE


Microsoft

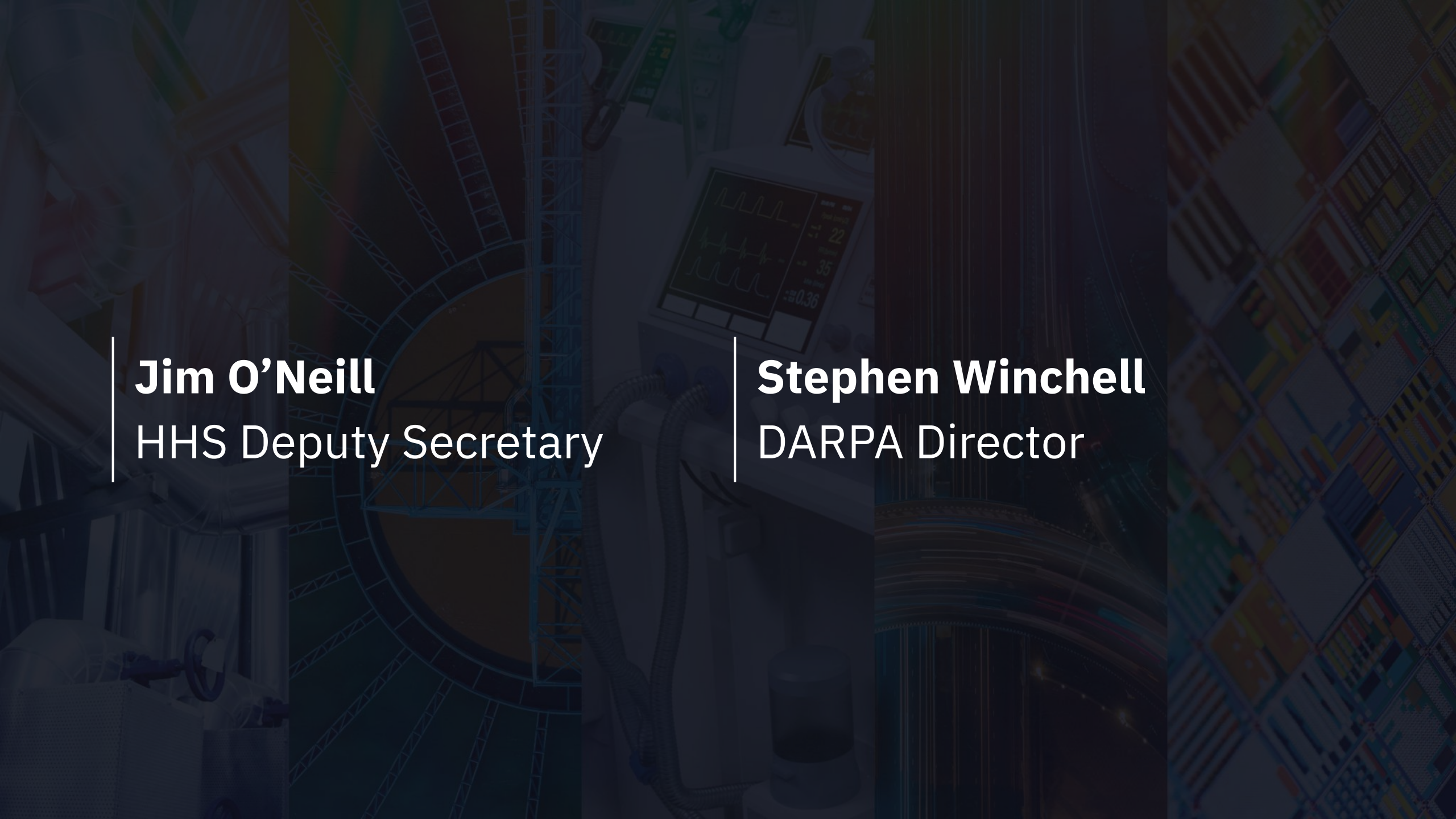

NIST


LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY


Mayhem


OpenAI

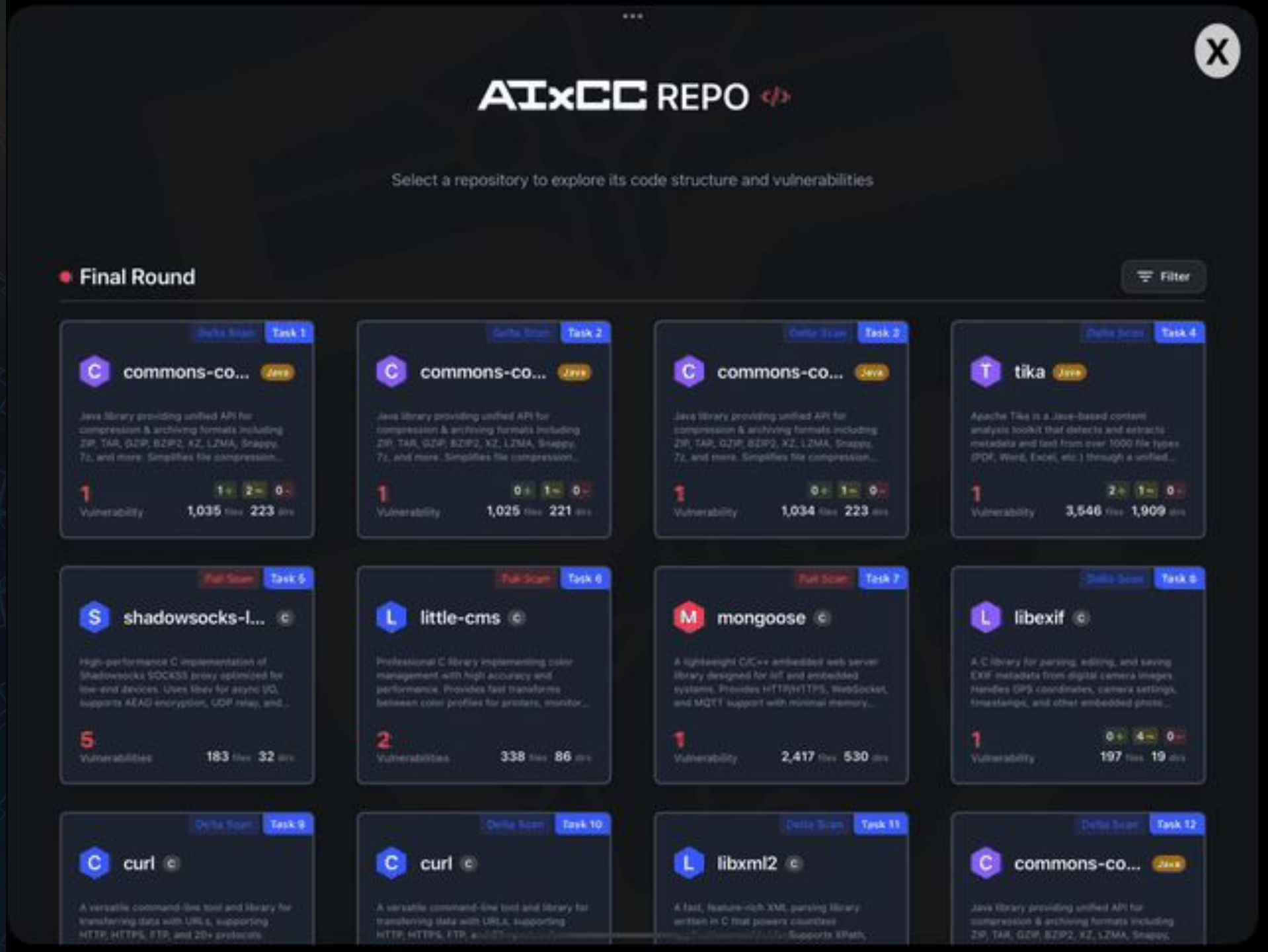

CMS.gov



Jim O’Neill
HHS Deputy Secretary

Stephen Winchell
DARPA Director

Repo Viewer



AIxCC
AI CYBER CHALLENGE

CRS Focus

42-b3yond-6ug
Last Action: Fuzzing

Team Atlanta
Last Action: Fuzzing

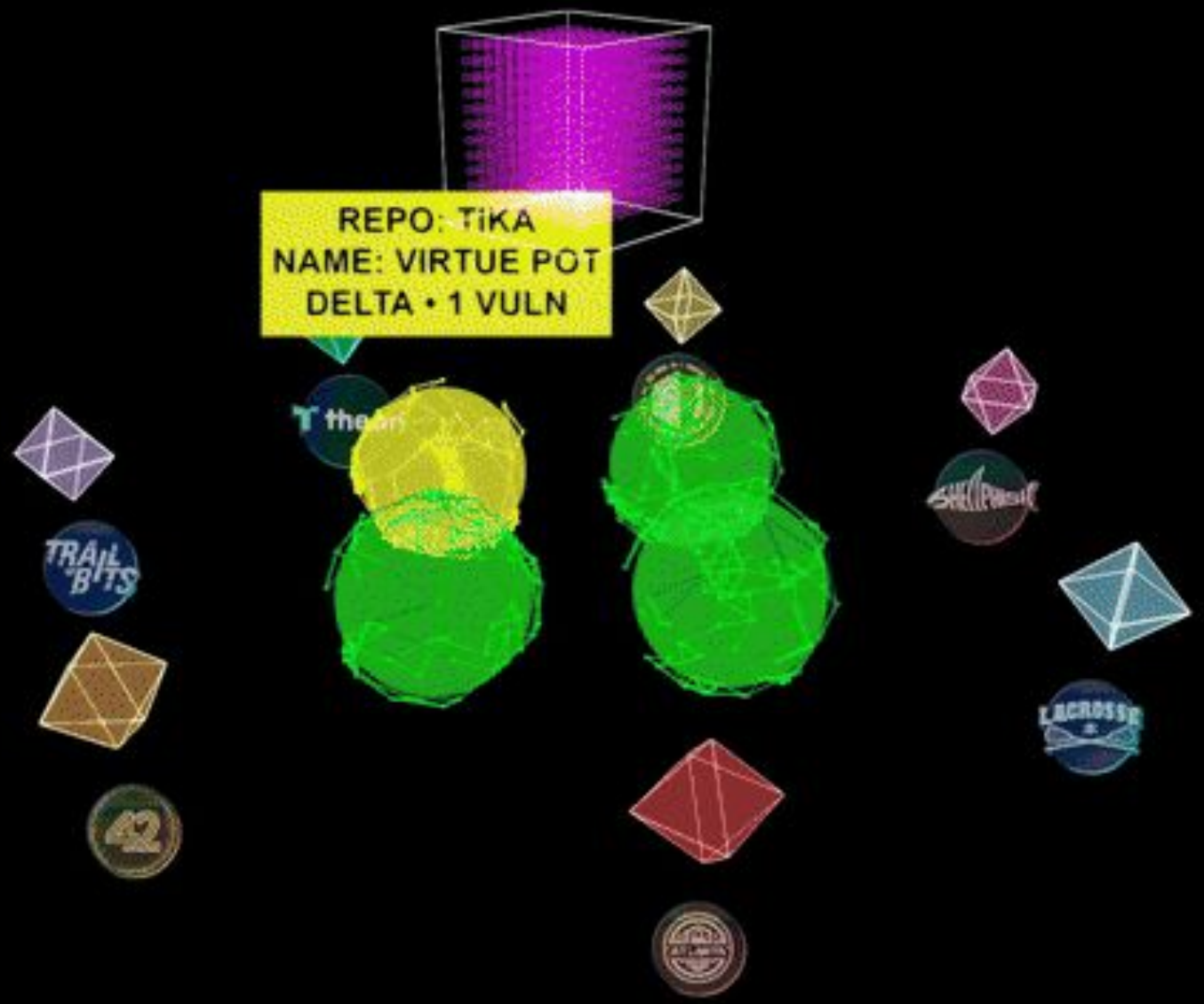
Theori
Last Action: Dynamic Analysis

Trail of Bits
Last Action: Input Generation

Lacrosse
Last Action: Building

All You Need IS A Fuzzing Brain
Last Action: Fuzzing

Shellphish
Last Action: Dynamic Analysis



DARPA + ARPA-H

AIxCC
AI CYBER CHALLENGE

What's Next @ DEF CON

AIxCC EXPERIENCE

- talk to teams
- view competition data / artifacts
- talk with collaborators
- talk with critical infra folks
- talk with related gov. project owners

What's Next

archive.aicyberchallenge.com

Release Timeline

- ➔ **NOW**: Shellphish, Team Atlanta, Theori, Trail of Bits (Competitor CRSs)
- ➔ **NOW**: Automated Harness Generation - SHERPA (github.com/AIxCyberChallenge/sherpa)
- ➔ **Aug 10**: All You Need IS A Fuzzing Brain (Competitor CRS)
- ➔ **Aug 24**: 42-b3yond-6ug, Lacrosse (Competitor CRSs)
- ➔ **Oct**: Competition Infrastructure, Challenge Repositories, Data, and Telemetry (pending disclosure to maintainers)

AIxCC
AI CYBER CHALLENGE

MAINTAINTERS (OSSF / OSTIF)

contact us to collaborate at
aixcc@darpa.mil

STORE

darpa-exchange-organization.square.site

POSTERS

aicyberchallenge.com/education/

DARPA / ARPA-H - Join Us!

https://www.darpa.mil/work-with-us

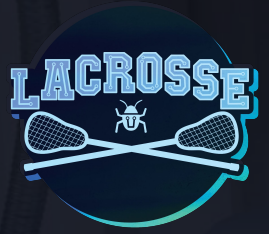
https://arpa-h.gov/

DARPA + ARPA-H

AIxCC

AI CYBER CHALLENGE

COMPETITOR HIGHLIGHTS



42-b3yond-6ug

"Czar of the SARIF"

Most correct SARIF assessments

"Giant Slayer"

Scored on a repo >5M LOC

Top 3 LLMs used:

- ➔ GPT-4.1
- ➔ Claude Opus 4
- ➔ Claude Sonnet 4

AIxCC
AI CYBER CHALLENGE

ALL YOU NEED IS A FUZZING BRAIN

"-Ofast"

First Blood:
C real world vuln

"Faster Than Pizza Delivery"

Score < 5 min
into a task

Top 3 LLMs used:

- ➔ GPT-4o
- ➔ Claude 3.7 Sonnet
- ➔ Claude Opus 4

AIxCC
AI CYBER CHALLENGE

Lacrosse

"Professional Assassin"

PoV success >95%

"Raiders of the Lost PoV"

Discovered a real world vuln

Top 3 LLMs used:

- ➔ GPT-4.1
- ➔ GPT-4.1 mini
- ➔ GPT-4o mini

AIxCC
AI CYBER CHALLENGE

Shellphish

"Best Telemetry"

Reporting LLM and CRS activity

"The Doctor is In"

Passing patch rate > 95%

Top 3 LLMs used:

- ➔ Claude Sonnet 4
- ➔ o4-mini
- ➔ Claude 3.7 Sonnet

AIxCC
AI CYBER CHALLENGE

Team Atlanta

“The Disruptor”

Most real world vulns discovered

“Bundle Baron”

Most scoring bundles

Top 3 LLMs used:

- → o4-mini
- → GPT-4o
- → o3

AIxCC
AI CYBER CHALLENGE

Theori

"Thrifty"

Least $$ spent per vuln patched

"Extra Caffeinated"

Most Java real world vulns discovered

Top 3 LLMs used:

- → o3
- → Claude Sonnet 4
- → o4-mini

AIxCC
AI CYBER CHALLENGE

Trail of Bits

"LOC Ness Monster"

Scored w/ patch diff > 300 LOC

"Cornucopia"

Scored on 20 unique CWEs

Top 3 LLMs used:

- ➔ Claude Sonnet 4
- ➔ GPT-4.1 mini
- ➔ GPT-4.1

AIxCC
AI CYBER CHALLENGE


AIxCC
AI CYBER CHALLENGE

CONGRATULATIONS TO TEAM

...

3rd PLACE

AIxCC AI CYBER CHALLENGE → $1,500,000

DARPA + ARPA-H

CONGRATULATIONS TO TEAM

theori

Theori

3rd PLACE

AIxCC AI CYBER CHALLENGE → $1,500,000

DARPA + ARPA-H


AIxCC
AI CYBER CHALLENGE

CONGRATULATIONS TO TEAM

...

2nd PLACE

AIxCC AI CYBER CHALLENGE → $3,000,000

DARPA + ARPA-H

CONGRATULATIONS TO TEAM

Trail of Bits

2nd PLACE

AIxCC AI CYBER CHALLENGE → $3,000,000

DARPA + ARPA-H


AIxCC
AI CYBER CHALLENGE

CONGRATULATIONS TO TEAM

...

1st PLACE

AIxCC AI CYBER CHALLENGE → $4,000,000

DARPA + ARPA-H

CONGRATULATIONS TO TEAM

Atlanta

1st PLACE

AIxCC AI CYBER CHALLENGE → $4,000,000

DARPA + ARPA-H

Scoreboard breakdown

Team	***Team Total Score***	% Correct Submission (r)	*Vulnerability Discovery Score (VDS)*	*Program Repaid Score (PRS)*	*SARIF Assessment Score (SAS)*	*Bundle Score (BDL)*
Team Atlanta (9caa56)	**392.76**	91.27%	79.71	171.10	5.99	136.38
Trail of Bits (309958)	**219.35**	89.33%	52.49	101.21	1.00	65.29
Theori (3fad2e)	**210.68**	44.44%	58.12	110.34	4.97	53.57
All You Need IS A Fuzzing Brain (1b9bb5)	**153.70**	53.77%	54.81	77.60	6.52	28.28
Shellphish (463287)	**135.89**	94.83%	47.94	54.31	8.47	25.29
42-b3yond-6ug (ee79d5)	**105.03**	89.23%	70.37	14.22	9.80	10.97
Lacrosse (e87a4d)	**9.59**	42.86%	1.68	5.43	0.00	3.62

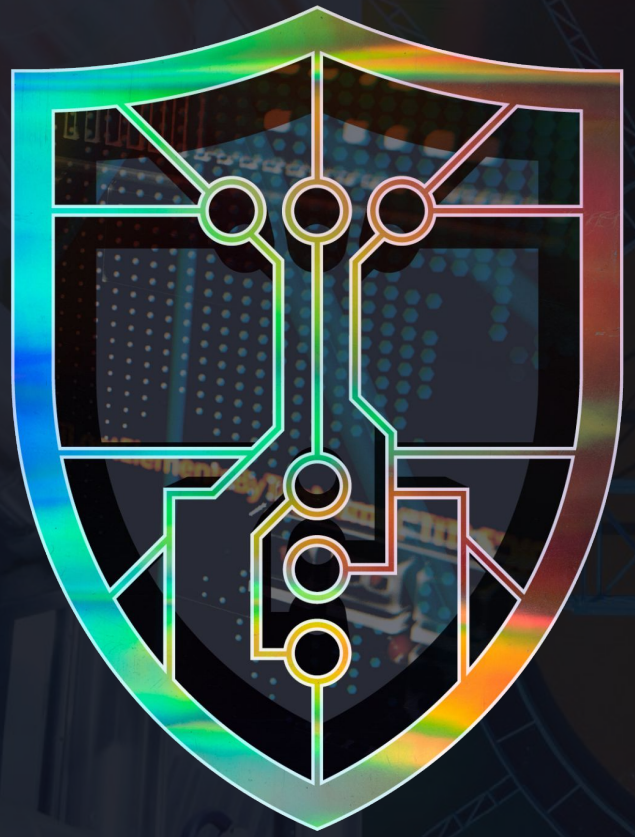
$$Team\ Score = \sum Challenge\ Scores$$

$$Challenge\ Score = AM * (VDS + PRS + SAS + BDL)$$

$$AM = 1 - (1 - r)^4$$

AIxCC
AI CYBER CHALLENGE

DARPA + ARPA-H



AIxCC
AI CYBER CHALLENGE

The world changes today.

Automated patch development is:

Fast
Scalable
Cost-effective
Available / Open-source

AI + CRS = The Future


AIxCC
AI CYBER CHALLENGE