Welcome to Auto-ISAC!

Monthly Virtual Community Call

July 1, 2020

"Teams Meeting Protocol"

[redacted]

Please Note…

1) The **Microsoft Teams meeting link** will provide both audio and visual presentation. In case you need to dial in for audio, please use the phone number and conference ID provided on the invite in the meeting invitation. If you are outside of the U.S, use "**Local Numbers**" link provided in the same meeting invite.
2) If you are dialing in for audio, **please press *6 to mute or unmute** your line.
3) Please keep your **mic muted** at all times, except when the host is addressing your request to ask a question or to provide feedback. Any background noise may disrupt the audio quality for other listeners.
4) If you have question or feedback, you can also use the **chat function**.
5) If you would like to speak, please use **raise hand function** on your screen. The host will be notified and will acknowledge you when ready.

Agenda

Time (ET)	Topic
11:00	**Welcome** ➢ Why we're here ➢ Expectations for this community
11:05	**Auto-ISAC Update** ➢ Auto-ISAC overview ➢ Heard around the community ➢ What's Trending
11:15	***DHS CISA Community Update***
11:20	**Featured Speaker:** **Tim Mackey, Principal Security Strategist, Synopsys, Cybersecurity Research Center (CyRC). *"2020 Open Source Security and Risk Analysis (OSSRA) Report"***
11:45	**Around the Room** ➢ Sharing around the virtual room
11:55	**Closing Remarks**

Welcome - Auto-ISAC Community Call!

Purpose: These monthly Auto-ISAC Community Meetings are an opportunity for you, our Members & connected vehicle ecosystem Partners, to:

- ✓ *Stay informed of Auto-ISAC activities*
- ✓ *Share information on key vehicle cybersecurity topics*
- ✓ *Learn about exciting initiatives within the automotive community from our featured speakers*

Participants: Auto-ISAC Members, Potential Members, Strategic Partners, Academia, Industry Stakeholders, and Government – *the whole of the automotive industry*

Classification Level: **TLP GREEN:** may be shared within the Auto-ISAC Community, and "off the record"

How to Connect: For further info, questions, or to add other POCs to the invite, please contact us! (fayefrancy@automotiveisac.com)

Engaging in the Auto-ISAC Community

❖ Join

- ❖ If your organization is eligible, apply for Auto-ISAC membership
- ❖ If you aren't eligible for membership, connect with us as a partner
- ❖ Get engaged – *"Cybersecurity is everyone's responsibility!"*

19 *Navigator Partners*

12 *Innovator Partners*

❖ Participate

- ❖ Participate in monthly virtual conference calls (1st Wednesday of month)
- ❖ If you have a topic of interest, let us know!
- ❖ Engage & ask questions!

20 *OEM Members*

❖ Share – *"If you see something, say something!"*

- ❖ Submit threat intelligence or other relevant information
- ❖ Send us information on potential vulnerabilities
- ❖ Contribute incident reports and lessons learned
- ❖ Provide best practices around mitigation techniques

36 *Supplier & Commercial Vehicle Members*

Membership represents **99%** *of cars on the road in North America*

Coordination with **23** *critical infrastructure ISACs through the National Council of ISACs (NCI)*

AUTO ISAC – 2020 WAY FORWARD

[redacted]

ROLES, RESPONSIBILITIES & METRICS | *Measuring Success*

VALUE STREAMS & PERFORMANCE INDICATORS

Top Line Goal: Zero safety related cyber events in the industry

INFO SHARING & AWARENESS	EDUCATION	RELATIONSHIPS
% Participation Sharing / Platform / Attendance	% Taking Educational Offerings Maturity Surveys	% Member Satisfaction with value added relationships

Bottom Line Goal: ***Automotive Cybersecurity Resiliency Across Industry!***

2020 Board of Directors

Executive Committee (ExCom)

Kevin Tierney
Chair of the Board of the Directors
GM

Josh Davis
Vice Chair of the Board of the Directors
Toyota

Jenny Gilger
Secretary of the Board of the Directors
Honda

Tim Geiger
Treasurer of the Board of the Directors
Ford

Todd Lawless
Chair of the Advisory Board
Continental

2020 Advisory Board (AB) Leadership

Todd Lawless
Chair of the Advisory Board
Continental

Brian Murray
Vice Chair of the Advisory Board
ZF

Kevin Walker
Chair of the SAG
Aptiv

Larry Hilkene
Chair of the CAG
Cummins

Member Roster

As of June 2, 2020

Highlighted = Change

Aisin	Honda	Oshkosh Corp
Allison Transmission	Hyundai	PACCAR
Aptiv	Infineon	Panasonic
AT&T	Intel	Qualcomm
Blackberry Limited	Kia	Renesas Electronics
BMW Group	Knorr Bremse	Subaru
Bosch	Lear	Sumitomo Electric
Continental	LGE	Tokai Rika
Cummins	Magna	Toyota
Denso	MARELLI	TuSimple
Delphi Technologies	Mazda	Valeo
FCA	Mercedes-Benz	Veoneer
Ford	Mitsubishi Motors	Volkswagen
Garrett	Mitsubishi Electric	Volvo Cars
General Motors	Mobis	Volvo Group
Geotab	Navistar	Waymo
Google	Nexteer Automotive Corp	Yamaha Motors
Harman	Nissan	ZF
Hitachi	NXP	TOTAL: 56

Auto-ISAC Activities

Auto-ISAC Updates

- **Advisory Board & Board of Directors Meeting Held Virtually *June 25th***
- **First official Audit Review *Completed!***
- **New Member added in June – *Nexteer Automotive Corporation***
- **Auto-ISAC Member Incident Response Plan (IRP) Reviews *Completed!***
- **Auto-ISAC Member 4 IRP Drills completed *Month of June***
- **Auto-ISAC Member TableTop Exercise (TTX) *Going Virtual***
- **Auto-ISAC Summit October 14-15th – registration, call for papers, and sponsorships on website – www.automotiveisac.com. *May be going virtual – standby for more details in July***

Auto-ISAC Summit – Oct 14-15th

AUTO-ISAC SUMMIT

GM

Oct. 14-15, 2020

Detroit, MI

2 days

400 attendees

ABOUT THE AUTO-ISAC SUMMIT:
The 2020 Auto-ISAC Summit hosted by General Motors connects global automotive industry insiders during two days of transformative conversations around cyber attack resilience and response.

Registration is Open | Call for Papers (due 6/30) | Sponsor Prospectus

Threat actors are demonstrating increased capabilities in industrial control system (ICS) and operational technology (OT) environments

EKANS Ransomware Palo Alto's Unit 42, Kaspersky ICS CERT, MalwareBytes, Dragos, and other cyber threat intelligence firms have analyzed an emerging ransomware strain that terminates processes and services associated with manufacturing and ICS control software. EKANS ransomware is named after its behavior of appending a hexadecimal string 'EKANS' to the ends of files before encrypting infected machines. According to Unit 42, "EKANS' intrusion vector at the moment seems to be spear phishing, to compromise credentials." Unit42 and MalwareBytes also suspect that open RDP processes may also be used for initial intrusion.

Security surprise: Four Zero-Days Spotted in Attacks on Researchers' Fake Networks Four new zero-day attacks were discovered when hackers employed them against fake systems set up by researchers studying hacking attempts on industrial systems. The attack types include denial-of-service and command-replay attacks. These vulnerabilities and associated exploits were disclosed to the device manufacturers.

Sodinokibi: Ransomware Attackers also Scanning for PoS Software, Leveraging Cobalt Strike
Symantec researchers have spotted a Sodinokibi targeted ransomware campaign in which the attackers are also scanning the networks of some victims for credit card or point of sale (PoS) software. It is not clear if the attackers are targeting this software for encryption or because they want to scrape this information as a way to make even more money from this attack. While many of the elements of this attack are 'typical' tactics seen in previous attacks using Sodinokibi, the scanning of victim systems for PoS software is interesting, as this is not typically something you see happening alongside targeted ransomware attacks. It will be interesting to see if this was just opportunistic activity in this campaign, or if it is set to be a new tactic adopted by targeted ransomware gangs.

For more information or questions please contact analyst@automotiveisac.com

CISA RESOURCE HIGHLIGHTS

Upcoming Events:

- ESF-14 (Long Term Community Recovery) COVID-19 Conference Calls:
  - Every first and third Tuesday of each month beginning July 7, 2020 from 3:00PM-4:15PM EST **until further notice**
  - Participant dial-in: 1-800-593-7177, Participant PIN: 7963614#
- National Business Emergency Operation Center (NBEOC) Conference Calls:
  - Mondays and Fridays at 3:00PM EST **until further notice**
  - Participant dial-in: 1-800-619-3427, Participant PIN: 2725748#
  - **No call this Friday, July 3, 2020**

TLP: WHITE – CISA Current Activity – ACSC Releases Advisory on Cyber Campaign Using Copy-Paste Compromises

- The Australian government became aware that they and a number of companies were being targeted by a sophisticated state-based actor.
- The actor was also found to be leveraging a number of initial access vectors, with the most prevalent being the exploitation of public-facing infrastructure.
- ACSC stated that two (2) key mitigations - prompt patching of internet-facing resources and the use of multi-factor authentication across all remote access services would have greatly reduced the risk of compromise by the TTPs identified in the advisory
- See https://www[.]cyber[.]gov[.]au/sites/default/files/2020-06/ACSC-Advisory-2020-008-Copy-Paste-Compromises.pdf and https://www[.]us-cert[.]gov/ncas/current-activity/2020/06/22/acsc-releases-advisory-cyber-campaign-using-copy-paste-compromises

TLP: WHITE - CISA Current Activity – Ripple20 Vulnerabilities

- Multiple vulnerabilities, collectively known as “Ripple20”, were found to affect TCP/IP stack implementations for embedded systems
- CISA issued Advisory ICSA-20-168-01 on June 18, 2020 to provide early notice of the reported vulnerabilities and identify baseline mitigations for reducing risks to these and other cybersecurity attacks
- The CISA advisory includes mitigation recommendations, and links to vendor-specific resources for affected products
- See https://www[.]us-cert[.]gov/ics/advisories/icsa-20-168-01 and https://www[.]us-cert[.]gov/ncas/current-activity/2020/06/16/ripple20-vulnerabilities-affecting-treck-ip-stacks for details

TLP: WHITE - CISA Current Activity – Palo Alto Networks Releases Security Updates for PAN-OS

- Security updates address a vulnerability affecting the use of Security Assertion Markup Language (SAML) in PAN-OS. An unauthenticated attacker with network access could exploit this vulnerability to obtain sensitive information.
- Update and workaround guidance is provided by the Palo Alto Networks Security Advisory for CVE-2020-2021
- See https://security[.]paloaltonetworks[.]com/CVE-2020-2021, https://www[.]us-cert[.]gov/ncas/current-activity2020/06/29/palo-alto-releases-security-updates-pan-os, and https://cve[.]mitre[.]org/cgi-bin/cvename.cgi?name=CVE-2020-2021 for details

TLP: WHITE - CISA Current Activity – Netgear Router Vulnerabilities

- Multiple Netgear router models contain vulnerabilities that a remote attacker can exploit to take control of an affected device.
- CISA encourages users and administrators to update to the most recent firmware version and to replace end-of-life devices that are no longer supported with security patches
- See the following for details:
  - https://www[.]us-cert[.]gov/ncas/current-activity/2020/06/29/netgear-router-vulnerabilities
  - https://www[.]kb[.]cert.org/vuls/id/576779
  - https://kb[.]netgear[.]com/000061982/Security-Advisory-for-Multiple-Vulnerabilities-on-Some-Routers-Mobile-Routers-Modems-Gateways-and-Extenders

TLP: WHITE – Additional Resources From CISA

- CISA Homepage - https://www[.]cisa[.]gov/
- CISA News Room - https://www[.]cisa[.]gov/cisa/newsroom
- CISA Publications Library - https://www[.]cisa[.]gov/publications-library
- CISA Cyber Resource Hub at https://www[.]cisa[.]gov/cyber-resource-hub
- CISA Vulnerability Management (formerly known as the National Cyber Assessment and Technical Services (NCATS) program) at https://www[.]us-cert[.]gov/resources/ncats/
- CISA Cybersecurity Directives - https://cyber[.]dhs[.]gov/directives/
- CISA COVID-19 Response – https://www[.]cisa[.]gov/coronavirus

For more information:
cisa.gov

Questions?
CISAServiceDesk@cisa.dhs.gov
1-888-282-0870


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY

Auto-ISAC Community Meeting

Why Do We Feature Speakers?

- These calls are an opportunity for information exchange & learning
- Goal is to educate & provide awareness around cybersecurity for the *connected vehicle*

What Does it Mean to Be Featured?

- Perspectives across our ecosystem are shared from members, government, academia, researchers, industry, associations and others.
- Goal is to showcase a rich & balanced variety of topics and viewpoints
- Featured speakers are not endorsed by Auto-ISAC nor do the speakers speak on behalf of Auto-ISAC

30+
Featured Speakers to date

How Can I Be Featured?

- If you have a topic of interest you would like to share with the broader Auto-ISAC Community, then we encourage you to contact us!

7 ***Best Practice Guides available on website***

2000+
Community Participants

Slides available on our website – www.automotiveisac.com

Featured Speaker

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Tim Mackey, Synopsys CyRC

Principal Security Strategist, Synopsys CyRC

Tim Mackey is a principal security strategist within the Synopsys CyRC (Cybersecurity Research Center). He joined Synopsys as part of the Black Duck Software acquisition where he worked to bring integrated security scanning technology to Red Hat OpenShift and the Kubernetes container orchestration platforms.

As a security strategist, Tim applies his skills in distributed systems engineering, mission critical engineering, performance monitoring, large-scale data center operations, and global data privacy regulations to customer problems. He takes the lessons learned from those activities and delivers talks globally at well-known events such as RSA, Black Hat, Open Source Summit, KubeCon, OSCON, DevSecCon, DevOpsCon, Red Hat Summit, and Interop.

Tim is also an O'Reilly Media published author and has been covered in publications around the globe including USA Today, Fortune, NBC News, CNN, Forbes, Dark Reading, TEISS, InfoSecurity Magazine, and The Straits Times.

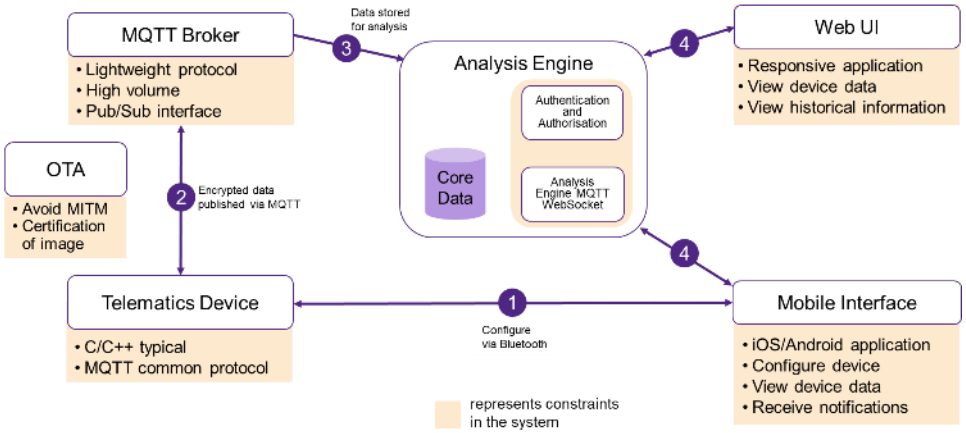
2020 Open Source Security and Risk Analysis Report

Learning from the Governance Decisions of Others

Tim Mackey, Principal Security Strategist,
Synopsys Cybersecurity Research Center

June 2020

Ideas are applications– Applications are systems



Modern application

=

Custom or proprietary code

+

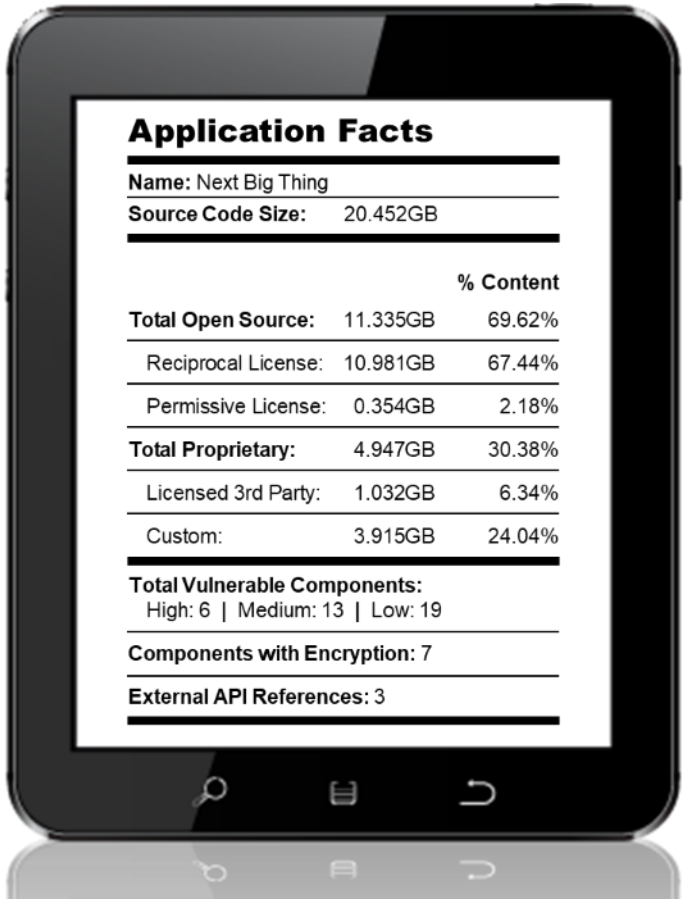
Open source components

+

API usage

+

Application behavior and configuration

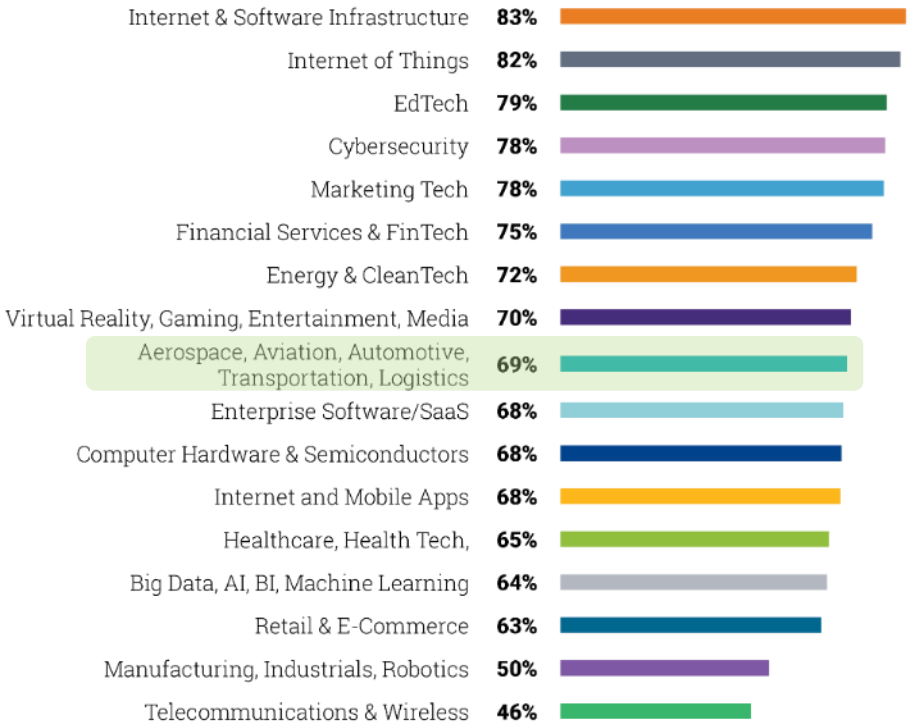


OSSRA Data from Due Diligence Audits of 1253 Codebases

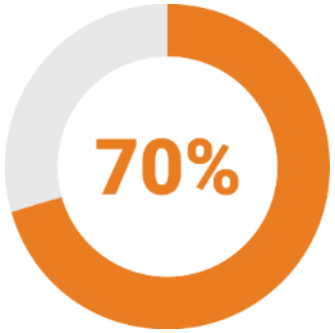
Industry	Distribution
Enterprise software/SaaS	27%
Healthcare, health tech, life sciences	11%
Internet and software infrastructure	10%
Financial services and fintech	6%
Cybersecurity	6%
Aerospace, aviation, automotive, transportation, logistics	5%
Internet and mobile apps	5%
Retail and e-commerce	4%
Virtual reality, gaming, entertainment, media	4%
Big data, AI, BI, machine learning	4%
Marketing tech	3%
Manufacturing, industrials, robotics	3%
EdTech	3%
Computer hardware and semiconductors	3%
Telecommunications and wireless	2%
Energy and cleantech	2%
Internet of Things	1%

Shared reuse and collaboration fuels innovation

Percentage of codebase which is open source



Codebases contained open source



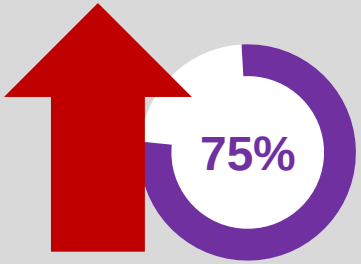
Average open source within codebase

Compliance hasn't kept up with usage

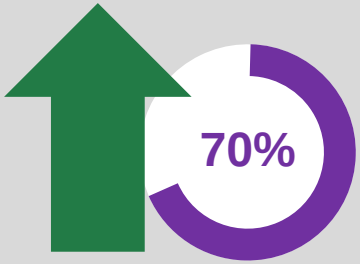
49% increase in components used to 445 per codebase

20 most popular open source licenses covered 98% of codebases

Open source license conflicts increased in 9 industries



Unpatched vulnerabilities increase 25%



Open source usage up 17%

Polymorphic code represented highest risk in OSSRA 2020

CVE-2018-16487, CVE-2019-10744, CVE-2018-14719

Components

Jackson-databind and Lodash

Core issue

- Jackson-databind 2.7.0+ implements a dynamic polymorphic binding model
- Multiple instances of prototype pollution in Lodash 4.17.12 and prior

Mitigation

Use explicit JSON schemas, binding models and objects without prototypes

Why multiple CVEs?

Jackson-databind top vuln in 2019: CVE-2018-7489, CVE-2017-7525 and CVE-2017-15095

Each CVE addressed different pollution paths and class types. Refactoring efforts didn't eliminate the core problems, but made it a bit easier to fix new instances.

Awareness is key to improvement

Rule #1: you can't patch what you don't know you have

- Patches must match source, so know your code's origin

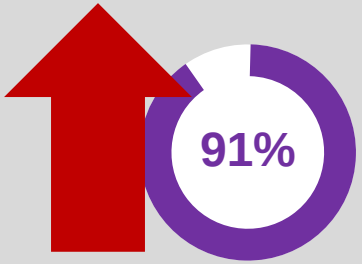
Open source isn't only about source, but about shared re-use

- Binary repositories simplify coding but exacerbate security

There is no vendor known as "open source"

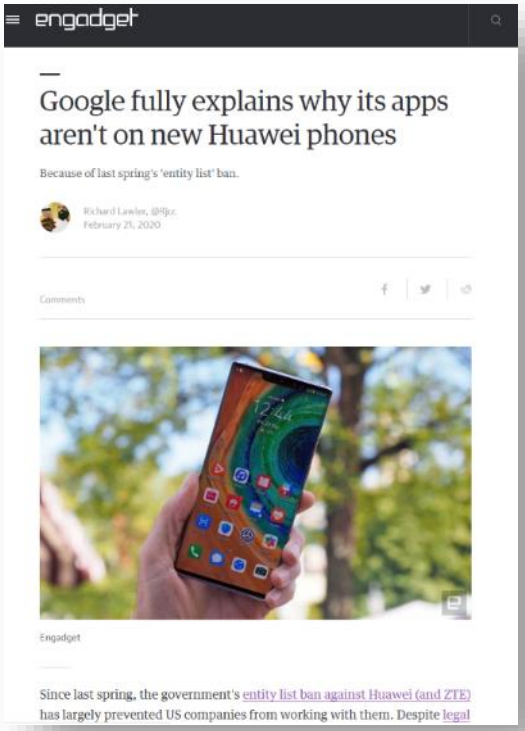
- Commercial security paradigms won't always work

Components per codebase



Contained obsolete or unmaintained components

Open source is mainstream with mainstream problems


engadget

Google fully explains why its apps aren't on new Huawei phones

Because of last spring's 'entity list' ban.

Richard Lawler, @Rjcr
February 21, 2020

Comments

Engadget

Since last spring, the government's entity list ban against Huawei (and ZTE) has largely prevented US companies from working with them. Despite legal


FORTUNE

SEARCH SIGN IN Subscribe Now

FINANCE
NBA's Los Angeles Lakers return $4.6M in PPP small business loans to the SBA

FINANCE
Whole Foods is restricting cash payments in some stores

FINANCE
IRS stimulus check portal: Try this trick if you are still getting 'payment status not available'

COMMENTARY
How the U.S. should invest in public health before reopening the economy

MAGAZINE · SILICON VALLEY

Oracle and Google are about to face off in tech's trial of the century

BY JEFF JOHN ROBERTS
February 17, 2020 6:30 AM EST

Oracle and Google will face off before the Supreme Court and that will have major complications for Silicon Valley.

PHOTO ILLUSTRATION BY EDMON DE HARO


Cockroach Labs

PRODUCT

Why We're Relicensing CockroachDB

Written by Peter Mattis, Ben Darnell and Spencer Kimball on June 4, 2019

Cockroach LABS

CockroachDB was conceived of as open source software. In the years since it first appeared on GitHub, we've tread a relatively typical path in balancing open source with creating a viable business. We've kept our core code under the Apache License version 2 (APL), launched a managed service, and gated some features for established companies under an enterprise license.

But our past outlook on the right business model relied on a crucial norm in the OSS world: that companies could build a business around a strong open source core product without a much larger technology platform company coming along and offering the same product as a service. That norm no longer holds.

Competitors have always been legally allowed to offer another company's OSS product as a service. Now, we're finally seeing it take place. We're witnessing the rise of highly-integrated providers take advantage of their unique position to offer "as-a-service" versions of OSS products, and offer a superior user experience as a consequence of their integrations. We've most recently seen it happen with Amazon's forked version of ElasticSearch, which Salil Deshpande neatly described in TechCrunch as both "self-interested and rational."

How can my team responsibly benefit from open source?

Open source software powers modern innovation

- Create a robust corporate strategy encompassing standards like ISO/SAE 21343
- Train all development and operations teams to identify critical component usage
- Recognize that open source is managed differently from commercial software

Open source governance starts with developers

- Train all developers to understand license implications
- Define patch and update strategy for usage aligned with ISO26262
- Inventory all software for open source usage – not just source code

Engage with your primary open source communities

- Open source is community led and vendor supported
- Communication of updates occurs at the community level
- Foster a sense of engagement and shared ownership within your teams
- Enhance collaboration skills inherent in distributed development

SYNOPSYS®

Build secure, high-quality software faster

Open Discussion

Any questions about the Auto-ISAC or future topics for discussion?

How to Get Involved: Membership

If you are an OEM, supplier or commercial vehicle, Carrier or Fleet, please join the Auto-ISAC!

- Real-time Intelligence Sharing
- Intelligence Summaries
- Regular intelligence meetings
- Crisis Notifications
- Member Contact Directory
- Development of Best Practice Guides
- Exchanges and Workshops
- Tabletop exercises
- Webinars and Presentations
- Annual Auto-ISAC Summit Event

To learn more about Auto-ISAC Membership or Partnership, please contact Auto-ISAC! contact.us@automotiveisac.com

Strategic Partnership Programs

Solutions Providers

For-profit companies that sell connected vehicle cybersecurity products & services.

Examples: Hacker ONE, SANS, IOActive, GRIMM

Associations

Industry associations and others who want to support and invest in the Auto-ISAC activities.

Examples: Alliance, ACEA, ATA, JAMA, CLEPA

Affiliations

Government, academia, research, non-profit orgs with complementary missions to Auto-ISAC.

Examples: DHS, NHTSA, Colorado State, Johns Hopkins, NCI

Community

Companies interested in engaging the automotive ecosystem and supporting the community.

Examples: Summit sponsorship – key events

INNOVATOR

Paid Partnership

- Annual investment and agreement
- Specific commitment to engage with ISAC
- In-kind contributions allowed

NAVIGATOR

Support Partnership

- Provides guidance and support
- Annual definition of activity commitments and expected outcomes
- Provides guidance on key topics / activities

COLLABORATOR

Coordination Partnership

- "See something, say something"
- May not require a formal agreement
- Information exchanges- coordination activities

BENEFACTOR

Sponsorship Partnership

- Participate in monthly community calls
- Sponsor Summit
- Network with Auto Community
- Webinar / Events

Auto-ISAC Benefits

- Focused Intelligence Information/Briefings
- Cybersecurity intelligence sharing
- Vulnerability resolution
- Member to Member Sharing

- Distribute Information Gathering Costs across the Sector
- Non-attribution and Anonymity of Submissions
- Information source for the entire organization
- Risk mitigation for automotive industry
- Comparative advantage in risk mitigation
- Security and Resiliency

Building Resiliency Across the Auto Industry

Thank you!

thank you
danke
рахмат
謝謝
ngiyabonga
شكراً جزيلاً
teşekkür ederim
gracias
Баярлалаа
спасибо
faafetai lava
mersi
kia ora
barka
welalin
tack
spas
dank je
misaotra
matondo
paldies
grazzi
mahalo
tapadh leat
vinaka
спасибі
blagodaram
kiitos
dankie
nanni
nandri
dhanyavad
mauruuru
köszönöm
hvala
gràcie
bayarlalaa
bedankt
enkosi
dziękuję
akun
dankon
ačiū
хвала
asante
manana
obrigada
tenki
murakoze
djiere dieuf
tau
mochchakkeram
дякую
mamnun
chokrane
chnorakaloutioun
gratias ago
gràcies
sulpáy
go raibh maith agat
sobodi
dėkuji
obrigado
mèsi
sagolun
sukriya
kop khun krap
taiku
arigatô
takk
dakujem
trugarez
didi madloba
kam sah hamnida
najis tuke
rahmat
ありがとう
terima kasih
tanemirt
rahmet
grazie
ευχαριστώ
diolch
dhanyavadagalu
shukriya
mercê
мерси
তোমাকে ধন্যবাদ
감사합니다
xièxie
merci

Our contact info

Faye Francy
Executive Director

20 F Street NW, Suite 700
Washington, DC 20001
703-861-5417
fayefrancy@automotiveisac.com

Sharmila Khadka
Executive Organizational Secretary

20 F Street NW, Suite 700
Washington, DC 20001
sharmilakhadka@automotiveisac.com

AUTO-ISAC
Automotive Information Sharing and Analysis Center

www.automotiveisac.com
@auto-ISAC