CYBERSECURITY
& Information Systems Digest

The Latest From the Cybersecurity & Information Systems Information Analysis Center // February 4, 2025

KNOWN EXPLOITED VULNERABILITIES (KEV) CATALOG

For the benefit of the cybersecurity community and network defenders—and to help every organization better manage vulnerabilities and keep pace with threat activity—the Cybersecurity & Infrastructure Security Agency (CISA) maintains the authoritative source of vulnerabilities that have been exploited in the wild. Organizations should use the KEV catalog as an input to their vulnerability management prioritization framework.

Learn more here: https://www.cisa.gov/known-exploited-vulnerabilities-catalog.

DID YOU MISS OUR LAST WEBINAR?

"A Multilayered Defense Strategy Against Adversarial AI Attack"

WATCH NOW!

or download the slides

NOTABLE TECHNICAL INQUIRY

What is the operational system risk imposed by the infrastructure deployment pipeline workflow?

Real-time data monitoring of systems and system forensics is an essential aspect to keeping your data security platform safe when relying on the use of Infrastructure as Code (IaC) and the potential vulnerabilities associated with its continuous deployment (CD). Many organizations are facing an information overload and are inadequately prepared for understanding and designing a cyber incident response plan with near-real-time monitoring,... **READ MORE**

UPCOMING WEBINAR


U.S. Army

Extended Reality for Maintenance and Repair...

February 19, 2025
12:00 PM – 1:00 PM

Presenter(s): *Joseph Matthew Friar* ***Host:*** *CSIAC*

Extended reality (XR) is an all-encompassing term that groups three similar technologies: (1) virtual reality (VR), (2) augmented reality (AR), and (3) mixed reality (MR). While XR is a field that has been in development in the U.S. Department of Defense (DoD) since the late 1960s, it has continued to see major advancements in recent years. This transformative technology has already made an impact across the DoD and holds considerable potential to... **READ MORE**

HIGHLIGHT

NSA Jointly Releases Recommendations for Closing the Software Understanding Gap

FORT MEADE, Md. – A report released by the National Security Agency (NSA), the Cybersecurity and Infrastructure Agency (CISA), the Defense Advanced Research Projects Agency (DARPA), and the Office of the Under Secretary of Defense for Research and Engineering (OUSD R&E) urges a national effort to better understand the behavior of software underpinning... **LEARN MORE**

EVENTS

Rocky Mountain Cyberspace Symposium 2025 (RMCS25)
February 10–13, 2025
Colorado Springs, CO

2025 DoD Cybersecurity & SAP IT Summit
February 10–13, 2025
North Charleston, SC

Homeland Security Cybersecurity and Infrastructure Conference
February 26–27, 2025
Atlanta, GA

Critical Infrastructure Protection & Resilience North America
March 11–13, 2025
Houston, TX

DoD Cyber Workforce Summit
March 20–21, 2025
Fort McNair, VA

18th Annual Homeland Security Week
March 25–26, 2025
Arlington, VA

Want your event listed here?
Email contact@csiac.org to share your event.

VOICE FROM THE COMMUNITY

David Pekala, MBA, PMP, GCIH, GSEC
Technical Director, NextGen Federal Systems, LLC

Dave Pekala supports the Army Analytics Solution to Establish Real-Time Operational Information Dominance Unified Data Reference Architecture effort as a data and Zero Trust subject matter expert. His focus is on information domination, digital transformation with DevSecOps, the StratusML platform for artificial intelligence, and Army intelligence systems. He supports modern systems engineering practices with digital engineering, including advanced modeling and simulation services supporting Joint Simulation Environment for weather effects.

ARE YOU A SME?

If you are a contributing member of the information systems community and are willing to help others with your expertise, you are a subject matter expert (SME).

Join our team today.

BECOME A SUBJECT MATTER EXPERT

ABOUT TECHNICAL INQUIRIES (TIs)

WHAT IS THE TI RESEARCH SERVICE?

- FREE service conducted by technical analysts
- 4 hours of information research
- Response in 10 business days or less

WHO CAN SUBMIT A TI?

- U.S. government (federal, state, or local)
- Military personnel
- Contractors working on a government or military contract

WHY UTILIZE THE TI RESEARCH SERVICE?

- Get a head start on your technical questions or studies
- Discover hard-to-find information
- Find and connect with other subject matter experts in the field
- Reduce redundancy of efforts across the government

To submit a TI, go to https://csiac.dtic.mil/technical-inquiries

FOR MORE: FOLLOW US ON SOCIAL


Getty Images

RECENT CSIAC TIs

- Are reinforcement learning techniques available for a next-generation threat system (NGTS)?
- Can information be provided on methods to efficiently improve commercial-off-the-shelf (COTS) information and communication technology (ICT) products for cybersecurity risks?
- Who can provide information on getting approval to use something like NotebookLM on closed-loop U.S. Department of Defense (DoD) computers?

RECENT DSIAC & HDIAC TIs

- Are there any service/government-funded laboratories currently developing hardened (anti-jam/anti-spoof) positioning, navigation, and timing and/or Global Positioning System packages for small unmanned aircraft systems?
- Is there a market survey of unattended ground sensors from commercial-off-the-shelf vendors?
- What multifunctional robotics platforms are used for first responder applications?

FEATURED NEWS

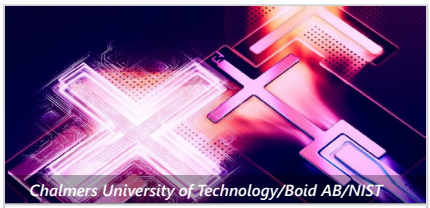
Data-Driven Innovations in AI/ML Capabilities Are Forging NETCOM's Future

FORT HUACHUCA, Ariz. — Under the leadership of the Data Science Directorate's director, Col. Michael Landin, the U.S. Army Network Enterprise Technology Command launched its new analytics... **READ MORE**

RECENT NEWS

Artificial Imagination

Brookhaven National Laboratory



Novel "Quantum Refrigerator" Is Great at Erasing Quantum Computer's Chalkboard

National Institute of Standards and Technology

Using AI to Rapidly Improve Acquisition Outcomes

Defense Acquisition University

Secure by Demand: Priority Considerations for Operational Technology Owners and...

CISA

Nimble Cellular Networks Keep Tactical Users Connected

Johns Hopkins Applied Physics Laboratory

CISA Publishes Microsoft Expanded Cloud Log Implementation Playbook

CISA

Cybersecurity

Knowledge Management & Information Sharing

Modeling & Simulation

Software Data & Analysis

4695 Millennium Drive Belcamp, MD 21017
443-360-4600 | contact@csiac.org |
csiac.dtic.mil Unsubscribe | Past Digests

CSIAC Cybersecurity & Information Systems Information Analysis Center