U.S. Fire Administration | FEMA

EMR-ISAC InfoGram Dec. 23 – Synthetic Opioids Master Question List released by DHS S&T; NFPA releases fifth Needs Assessment of US Fire Service

EMR-ISAC sent this bulletin at 12/23/2021 01:20 PM EST

View as a webpage / Share

Emergency Management and Response - Information Sharing and Analysis Center (EMR-ISAC)

The InfoGram

Volume 21 — Issue 50 | December 23, 2021

DHS S&T releases Synthetic Opioids Master Question List for response and research communities

The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) has just released a new Master Question List (MQL) for Synthetic Opioids (Opioid MQL). The Opioid MQL is a reference guide providing safety and operational considerations for the response community and current knowledge gaps for the research community. The document will serve as a living repository of ongoing research on synthetic opioids and will be periodically updated as new knowledge becomes publicly available.

Opioid drug overdose deaths in the United States are at a record high, with synthetic opioids like illicit fentanyl largely responsible. According to a recent analysis of the provisional CDC data on drug overdose deaths in 2021, fentanyl overdoses now comprise the leading cause of death for adults between the ages of 18 and 45, surpassing motor vehicle accidents, COVID-19, suicide, and cancer.

Exposure to these synthetic opioids presents unique and significant challenges to first responders. The compounds are highly toxic, deadly, and aerosols may remain at the scene well after responders arrive. Developing safe decontamination protocols, effective personal protective gear and detection equipment is an ongoing challenge.

To address this issue, DHS S&T's new Opioid MQL offers emergency responders current, consolidated, scientifically vetted information on the hazards of synthetic opioids. Topics

Highlights

addressed in the Opioid MQL include physical properties, routes of exposure, personal protective equipment, decontamination and destruction methods, detection technologies, and medical countermeasures. Safety and operational considerations are listed for each of these topics. The information provided is supported with extensive reference citations.

The new MQL was developed by DHS S&T's Chemical Security Analysis Center (CSAC) and the Office of Mission and Capability Support's Opioid Detection Program, in collaboration with DHS S&T's Hazard Assessment and Characterization Technology Center (HAC-TC) and the Probabilistic Analysis for National Threats and Hazards and Risks (PANTHR).

The current version of the Opioid MQL focuses on synthetic opioids commonly found in the illicit drug trade. More synthetic opioids will be added as information becomes available. Additional information, such as classified annexes, will be made available upon request.

To request support related to this document, contact DHS S&T CSAC at csacinfo@st.dhs.gov.

(Source: DHS S&T)

U.S. Fire Administration

The U.S. Fire Administration operates the Emergency Management and Response – Information Sharing and Analysis Center (EMR-ISAC).

For information regarding the EMR-ISAC visit www.usfa.dhs.gov/emr-isac or contact the EMR-ISAC office at: (301) 447-1325 and/or fema-emr-isac@fema.dhs.gov.

Subscribe here

NFPA releases fifth Needs Assessment of US Fire Service

Roles and responsibilities of fire departments continue to expand with no sign of stopping. From wildland urban interface (WUI) fires and active shooter incidents to hazardous materials response and traffic control duties, fire departments are being asked to do more and more, but in many cases, without the resources to support their needs.

On Dec. 14, the National Fire Protection Association (NFPA) released its Fifth U.S. Needs Assessment of the U.S. Fire Service. This report is published every five years and reflects the results of a survey sent to most U.S. fire departments. A total of 2,969 fire departments responded to the survey, beginning in 2020 and concluding in 2021, with approximately 75% responding online and 25% filling out the paper version. Overall, the response rate was 11%.

The survey includes a broad range of questions that work to identify where U.S. fire departments are experiencing gaps in equipment, staffing, and training, among other needs and resources.

Findings from this year's report show both progress and continued gaps in U.S. fire departments' needs and resources. Fire service needs are extensive across the board, and in nearly every area of need, the smaller the community protected, the greater the need. While some needs have been met in the years between the previous survey and this survey, many have been constant or have increased. Today, many fire departments are unable to fully staff engines, fully train their members for structural and wildland firefighting, or provide all their firefighters with personal protective clothing and updated self-contained breathing apparatus (SCBA).

The following are highlighted findings from the NFPA's fifth fire service needs assessment:

- Across every response type covered in the survey, from structural firefighting to active shooter situations, there are fire department personnel responsible for responding to incidents for which they have not been formally trained or certified.

- Behavioral health programs are a critical area of unmet need.
- Positive trends in the availability and use of personal protective clothing and equipment have been tempered by ongoing challenges with older equipment, other unmet needs, and maintenance challenges.
- Community risk reduction remains a challenge.

The NFPA will be working on additional state-level reporting in the coming months to produce these types of reports for selected states, as has been done for Needs Assessment reports in previous years.

The NFPA's Fifth U.S. Needs Assessment Report is free and available to download from the NFPA's website. An interactive viewer of all survey data from this fifth Needs Assessment can be found here: www.nfpa.org/5thneedsresults.

(Source: NFPA)

New interactive online IPAWS Toolkit for planning an alerts, warnings and notifications program

For public safety agencies, having an effective program for public alerts, warnings and notifications is a cornerstone of good emergency and disaster response.

Last month, the Federal Emergency Management Agency (FEMA) and the Department of Homeland Security (DHS) Science & Technology Directorate (S&T) released an interactive, web-based version of the Integrated Public Alert and Warning System (IPAWS) Program Planning Toolkit which builds on the document-based version of the toolkit released in September 2020.

Today, more than 1,500 federal, state, local, tribal and territorial alerting authorities use IPAWS to send critical emergency updates in their jurisdictions. IPAWS can be used to send multiple types of emergency alerts—from Wireless Emergency Alerts (WEA) on mobile devices and digital highway signs to the Emergency Alert System, which delivers alerts over the radio and television—all geotargeted with critical news based on a person's geographic location.

The new toolkit is designed to aid alerting authorities and alert originators at federal and state, local, tribal, and territorial (SLTT) levels in developing an Alerting Program Plan using best practices.

The interactive toolkit walks the user through an alerting plan template in five steps. At each step, users are prompted to gather and enter information about their agency's current plans and capabilities. Each prompt is accompanied by guidance, instructions, and sample response text to model what the user might enter for their own agency. The final result is a downloadable, formatted draft of a comprehensive alerting plan tailored to their agency's operational capabilities.

Before an emergency occurs, it is critical that alerting authorities and alert originators have messaging templates saved for various scenarios, to save time during a disaster or emergency. To address this, the toolkit includes a message template creator that walks a user through the research-based recommended format for critical alert messaging. The toolkit is also supported by a set of sample templates for alert messages for a variety of scenarios, in Spanish and English language translations.

FEMA estimates it will take approximately two hours to complete all five steps in the interactive toolkit; however, the exact timeframe is dependent on the user's familiarity with their agency's alerts, warnings, and notifications program. Once started, the user's responses to the steps are stored in their browser for 14 days. This allows them to stop and return to completing the plan using the same browser on the same computer. Clearing the browser's cache will remove the user's entries.

The new toolkit also includes an updated list of Frequently Asked Questions about IPAWS.

To learn more about the new toolkit and to try the new web-based forms to draft your agency's Alerting Program Plan, visit FEMA's IPAWS Program Planning Toolkit page.

(Source: FEMA)

Webinar: State of 911 series - Impacts of incident-related imagery in ECCs and NG911 success in Washington State with civilian-military PSAP integration

The National 911 Program will hold a webinar in its State of 911 series on **Tues., January 11, at 12:00 p.m. EST**. The webinar will discuss the impacts of incident-related imagery in emergency communications centers (ECCs) and participants will learn about the latest chapter of the Next Generation 911 (NG911) Interstate Playbook, which addresses the state of Washington's successful interconnection of civilian and military Public Safety Answering Points (PSAPs).

New technologies in ECCs are enabling the public to exchange multimedia such as photos, videos and text messages with 911 call takers. This information can improve situational awareness and inform emergency response efforts; however, the data may also impact operations, resources, and personnel when telecommunicators must analyze multimedia during voice calls, communicate through text messages and/or conduct video calls with the public.

This session will discuss emerging technologies in ECCs and considerations for addressing incident-related imagery, such as establishing data management policies and procedures, assessing training and educational requirements, supporting staff wellness and evaluating recruitment and retention guidelines. Participants will also learn about resources to help plan for receiving multimedia in their center, such as the SAFECOM and National Council of Statewide Interoperability Coordinators (NCSWIC) Incident-Related Imagery Impacts 101 document.

The second session of the webinar will discuss Chapter 5 of the NG911 Interstate Playbook. This chapter highlights the collaboration in Washington State between local, military, and state agencies to successfully interconnect civilian and military PSAPs. Presenters from the state, Pierce County, and Joint Base Lewis-McChord (JBLM) will explain their collaborative efforts to plan and integrate JBLM 911 communications with the county 911 system to create an interoperable regional solution for NG911 core services and an ESInet. Join this session to learn more about the lessons they learned and the advice they can offer.

The webinar is free and open to all interested, but registration is required. A recording and slide deck will be made available soon after the webinar.

The recordings and slide decks from all previous webinars in the National 911 Program's State of 911 series are available online. For information about future webinars, you can sign up for email alerts.

(Source: National 911 Program)

Cyber Information and Incident Assistance Links

MS-ISAC
SOC@cisecurity.org
1-866-787-4722

IdentityTheft.gov

IC3

Cybercrime Support Network

General Information Links

StopRansomware.gov

FTC scam list

CISA alerts

Law Enforcement Cyber Center

TLP Information

CISA, FBI, NSA and international partners issue advisory to mitigate Apache Log4j vulnerabilities

The Cybersecurity and Infrastructure Security Agency (CISA), along with the Federal Bureau of Investigation (FBI), National Security Agency (NSA), Australian Cyber Security Centre (ACSC), Canadian Centre for Cyber Security (CCCS), Computer Emergency Response Team New Zealand (CERT NZ), New Zealand National Cyber Security Centre (NZ NCSC), and the United Kingdom's National Cyber Security Centre (NCSC-UK) issued a joint cybersecurity advisory with technical details, mitigations, and resources to address known vulnerabilities in the Apache Log4j software library. This advisory provides critical guidance that any organization using products with Log4j should immediately implement.

The joint advisory is in response to the active, worldwide exploitation by numerous threat actors, including malicious cyber threat actors, of vulnerabilities found in the widely used Java-based logging package Log4j.

CISA created a dedicated Log4j webpage to provide an authoritative, up-to-date resource with mitigation guidance and resources for network defenders, as well as a community-sourced GitHub repository of affected devices and services. Organizational leaders should also review NCSC's blog post, "Log4j vulnerability: what should boards be asking?," for information on Log4Shell's possible impact on their organization as well as response recommendations.

This is an evolving situation; therefore, this advisory will be updated as we learn and assess new information. Read the full joint cybersecurity advisory.

(Source: CISA)

Google finds 35,863 Java packages using defective Log4j

The computer security industry is bracing for travel on long, bumpy roads littered with Log4j security problems as experts warn that software dependency patching hiccups will slow global mitigation efforts.

The sheer scale and impact of the crisis became a bit clearer this week with Google's open-source team reporting that a whopping 35,863 Java packages in Maven Central are still using defective versions of Log4j library. *(Editor's note: Maven Central is the largest and most significant Java package repository).*

Among the 35,863 vulnerable Java artifacts on Maven Central, the Google team found that direct dependencies account for around 7,000 of the affected artifacts. The majority of affected artifacts come from indirect dependencies, the researchers explained.

(Source: Security Week)

Critical Apache HTTPD server bugs could lead to RCE, DoS

It's got nothing to do with Log4Shell, except it may be just as far-reaching as Log4j, given HTTPD's tendency to tiptoe into software projects.

Apache, the open-source software foundation behind the Log4j logging library that's been making for so many Log4Shell headlines, on Monday put out an update to fix the two bugs in HTTPD, which is a web server that's right up there with Log4j in its ubiquity. Just like Log4j, HTTPD has a habit of getting itself quietly included into software projects, for example as part of an internal service that works so well that it rarely draws attention to itself, or as a component built unobtrusively into a product or service you sell that isn't predominantly thought of as "containing a web server."

Both vulnerabilities are found in Apache HTTP Server 2.4.51 and earlier.

CISA announced on Dec. 22 that the Apache Software Foundation has released Apache HTTP Server 2.4.52. This version addresses these vulnerabilities—CVE-2021-44790 and CVE-2021-44224—one of which may allow a remote attacker to take control of an affected system. CISA encourages users and administrators to review the Apache announcement and update as soon as possible.

(Sources: threatpost, CISA)

A cyber attack may have exposed information of thousands of Suffolk County first responders

A Suffolk County, New York vendor has reported a ransomware attack that could have exposed the personal information of thousands of first responders.

Suffolk IT workers don't know if the county's payroll information was exposed in the attack on UKG, the maker of the popular HR system Kronos. The county hasn't fully rolled out its use of the system. What is known is that the contact information for 3,900 police, sheriff deputies and emergency workers was entered into the system and that the company was hit on Saturday, Dec. 11 with a ransomware attack. Now, police officials are extremely concerned while lawmakers demand answers.

(Source: WSHU Long Island News)

Honolulu Board of Water Supply, Emergency Medical Services report cyberattacks on employee data

The time-keeping system Honolulu Emergency Medical Services (EMS) uses for employees was hit by a ransomware attack Sunday night, the third cyber intrusion of county networks since Thursday. EMS uses the same third-party system from the company Kronos as the Honolulu Board of Water Supply uses. The EMS' Kronos payroll system remains inoperable and supervisors are using manual time-keeping forms for employees.

(Source: Honolulu Star Advertiser)

CISA and FBI launch holiday cyber safety PSA

CISA, in partnership with the FBI, launched a joint public service announcement (PSA) on Dec. 20, sharing clear actions to stay cybersecure this holiday season. While staffing is low and offices are closed during the holidays, and with the recent disclosure of severe vulnerabilities in the widely used "log4j" software library, bad actors are actively seeking to take advantage of vulnerabilities inside organizations' networks and systems. This PSA is based on observations on the timing of high impact cyber incidents that have occurred previously rather than a reaction to specific threat reporting.

In light of persistent and ongoing cyber threats, CISA also released an Insights publication urging critical infrastructure owners and operators to take immediate steps to strengthen their computer network defenses against potential malicious cyberattacks.

(Source: CISA)

Note: The InfoGram will not be published on Thursday, Dec. 30 due to the federal holiday. It will resume on Thursday, Jan. 6.

The InfoGram is distributed weekly to provide members of the Emergency Services Sector with information concerning the protection of their critical infrastructures.

Fair Use Notice:
This InfoGram may contain copyrighted material that was not specifically authorized by the copyright owner. The EMR-ISAC believes this constitutes "fair use" of copyrighted material as provided for in section 107 of the U.S. Copyright Law. If you wish to use copyrighted material contained within this document for your own purposes that go beyond "fair use," you must obtain permission from the copyright owner.

Disclaimer of Endorsement:
The appearance of external hyperlinks does not constitute endorsement of the linked websites or the information, products or services contained therein. Reference to any specific commercial products, process or service by trade name, trademark, manufacturer or otherwise, does not necessarily constitute or imply its endorsement, recommendation or favoring by the EMR-ISAC or the U.S. government.

Section 504 Notice:
Section 504 of the Rehabilitation Act requires that FEMA grantees provide access to information for people with disabilities. If you need assistance accessing information or have any concerns about access, please contact FEMAWebTeam@fema.dhs.gov.
