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

The InfoGram

Volume 21 — Issue 27 | July 8, 2021

Fireshed Registry helps address the growing wildfire threat

Since 2015, the United States has experienced, on average, roughly 100 more large wildfires every year than the year before. This has created conditions in which wildfires overwhelm response capabilities.

On June 30, the White House released a statement summarizing the actions it is already taking, and those it intends to take once the FY2022 budget is passed, to address the growing wildfire threat. The statement acknowledges that management of wildfires is a multi-agency effort, requiring a risk-based suppression strategy. The statement highlights many of the valuable initiatives and projects already underway to manage wildfire risks and to facilitate safe and effective wildland firefighting.

One such project is the United States Forest Service's (USFS') Fireshed Registry. In May 2021, the USFS published a report describing the development and application of the Fireshed Registry in wildfire risk management. The Fireshed Registry is a geospatial dashboard and decision tool built in ArcGIS online, serving as the data warehouse for the Forest Service Scenario Planning Platform. Although the Fireshed Registry is not a public-facing application, its capabilities and plans for its continued development are described in detail in the report.

Just as watersheds are geographic delineations to manage water resources, and airsheds are delineated to manage air quality, firesheds are geographical areas, or "containers" delineated to manage wildfire risk within the wildland urban interface (WUI).

The Fireshed Registry's method of classifying wildfire risk offers advantages over existing tools and classification systems. Most existing WUI classification schemes rely on vulnerabilities within individual communities, such as the locations of structures and surrounding vegetation in the developed area.

The "fireshed" classification system is useful in addressing the current wildfire threat. Longer fire seasons and the rising size and severity of wildfires has made it necessary to prioritize large areas of wildlands - the source of fire in developed areas - rather than focusing solely on individual communities that need protection from these sources of fire.

Highlights

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

More importantly, the Fireshed Registry provides the Forest Service with a planning framework for tracking changes in fireshed conditions at forest, regional and national scales. This in turn provides a foundation for communication and coordination with external agencies and partners for cross-boundary collaboration, supporting the Shared Stewardship initiative.

The data from the Fireshed Registry, as part of the Forest Service Scenario Planning Platform, has many applications for improved resource and funding allocation, such as the ability to prioritize forest treatment projects, to allow for more efficient investment in hazardous fuels treatments, and to support alignment of local wildfire management priorities with national priorities.

(Source: USFS)

Project Jack Rabbit assesses chemical threats with rapid, large-scale chemical release trials

Each year, hundreds of millions of tons of toxic industrial chemicals like chlorine and ammonia are transported through U.S. population centers. Although these chemicals are essential, they are toxic and pose a risk to the public through accidental release or an act of terrorism.

To better understand and address this risk, the Department of Homeland Security (DHS) Science and Technology Directorate's (S&T's) Chemical Security Analysis Center (CSAC) launched Project Jack Rabbit in 2010. Prior to Project Jack Rabbit, large-scale releases of chlorine and anhydrous ammonia had never been tested at volumes representative of rail cars, tanker trucks, barges or bulk storage tanks.

The first phase of the project, Jack Rabbit I, involved outdoor releases of one- and two-ton quantities of chorine and anhydrous ammonia in 10 trials occurring in April and May of 2010. The final test report of CSAC's Jack Rabbit I was published in 2011.

The Jack Rabbit II test was designed to safely replicate accidental or intentional releases of chlorine gas from pressurized tanks and to document the downwind movement of the gas through an urban setting and in an open area. The Jack Rabbit II report was published in 2017.

The project impacts from Jack Rabbit II included:

- Improved chemical hazard modeling.
- Better planning for release incidents.
- More effective emergency response.
- Improved mitigation measures to reduce the impact to affected populations and infrastructure.
- Improved HazMat and industrial safety.
- Improved guidance and data for emergency response procedures and validation of protective action distances.

The third phase of this project, Jack Rabbit III, is currently in its early stages. Advanced concept technology demonstrations for small-scale releases of ammonia are scheduled for October 2021 at Dugway Proving Ground in the Utah desert. Large-scale anhydrous ammonia outdoor

releases, currently scheduled for 2023-2024, will represent high-risk surface transportation incidents.

(Source: DHS S&T)

CISA and FBI launch Operation Flashpoint to raise awareness about how to prevent bomb making

The Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Justice's Federal Bureau of Investigation (FBI) recently announced a new pilot program called "Operation Flashpoint." This program is intended to build awareness in communities across the U.S. about how to prevent bomb attacks.

Improvised Explosive Devices (IEDs) pose a significant threat in the United States. In 2020 alone, there were 2,061 total bomb threat, suspicious package, and device-related incidents across the nation, according to CISA's Office for Bombing Prevention TRIPwire report.

Major bombings can cause mass casualty events and cost hundreds of millions of dollars or more. Domestic violent extremists and others can build IEDs from common household items found at retail stores across the country. Approximately 250,000 businesses in the U.S. sell, use or distribute materials that can be used to build bombs.

The 90-day Operation Flashpoint pilot, which was launched on June 30 with an event in Clinton, Mississippi, will include events in other cities, including Columbia, South Carolina; Louisville, Kentucky; and Orlando/Tampa, Florida. The pilot seeks to reduce the threat of IED attacks by helping businesses detect the illegitimate acquisition, theft, or diversion of dangerous chemicals. The program encourages businesses and the public to voluntarily report suspicious activities, such as buying large amounts of chemicals and materials that can be used to build bombs.

See the full news release from CISA for more information. You can follow #OperationFlashpoint through the summer on Twitter: @CISAgov and @CISAInfraSec.

(Source: CISA)

NIST 2021 Disaster Resilience Symposium, July 20 and 21

Buildings, bridges, and other man-made structures are supposed to be safe. But sometimes they fail, due to various natural and human causes such as fire, earthquakes, high winds, errors in design and construction, flaws in materials, and even terrorist attacks.

The Engineering Laboratory at NIST will be hosting its fourth annual Disaster Resilience Symposium as a free, virtual only event on **July 20 and 21, 2021**, **from 11:00 a.m. to 3:30 p.m. EST.** The event will feature Disaster Resilience Grant Research Program recipients from 2019. These grant awardees conducted research related how earthquakes, wind and fire affect the built environment. This research can inform building designs, codes and standards to help those structures better withstand such hazards.

Topics for presentations during the symposium fall into the following areas:

- Disaster and Failure Studies.
- The National Earthquake Hazards Reduction Program.
- Wind Impact Reduction.
- Reduced Ignition of Building Components in Wildland-Urban Interface (WUI) Fires Project.

Visit NIST's website for more information, view a detailed agenda, and register for the event by filling out a brief registration form.

Capacity is limited, so **register before July 19** to help guarantee your spot. More information will be added to the website as it becomes available.

(Source: NIST)

Cyber Information and Incident Assistance Links

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

IdentityTheft.gov

IC3

Cybercrime Support Network

General Information Links

FTC scam list

CISA alerts

Law Enforcement Cyber Center

TLP Information

Kaseya ransomware attack: Your questions answered

It appears that attackers have carried out a supply chain ransomware attack by leveraging a vulnerability in Kaseya's VSA software against multiple managed service providers (MSP) -- and their customers. Customers were notified of the breach via email, phone, and online notices.

The FBI described the incident succinctly: a "supply chain ransomware attack leveraging a vulnerability in Kaseya VSA software against multiple MSPs and their customers." The vendor has also provided an in-depth technical analysis of the attack.

A security expert said the ransomware was pushed via an automated, fake, and malicious software update using Kaseya VSA dubbed "Kaseya VSA Agent Hot-fix". As of July 6, the estimate of customers impacted by the attack is between 50 direct customers, and between 800 and 1,500 businesses down the chain.

See the latest CISA-FBI Guidance for MSPs and their Customers Affected by the Kaseya VSA Supply-Chain Ransomware Attack for additional awareness and recommended actions.

(Source: ZDNet)

NSA-CISA-NCSC-FBI Joint Cybersecurity Advisory on Russian GRU Brute Force Campaign

The National Security Agency (NSA), Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and the United Kingdom's National Cyber Security Centre (NCSC) have released Joint Cybersecurity Advisory (CSA): Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments.

The CSA provides details on the campaign, which is being conducted by the Russian General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS).

CISA strongly encourages users and administrators to review the Joint CSA for GTSS tactics, techniques, and procedures, as well as mitigation strategies.

(Source: CISA)

PrintNightmare, critical Windows print spooler vulnerability

The CERT Coordination Center (CERT/CC) has released a VulNote for a critical remote code execution vulnerability in the Windows Print spooler service. CISA encourages administrators to disable the Windows Print spooler service in Domain Controllers and systems that do not print. Additionally, administrators should employ the following best practice from Microsoft's how-to guides, published January 11, 2021

For new information and mitigations, see Microsoft's updated guidance for the Print spooler vulnerability (CVE-2021-34527)

(Source: CISA)

Rural Alabama electric cooperative hit by ransomware attack

Wiregrass Electric Cooperative provides power in rural southeastern Alabama and was hit by a ransomware attack. Customers temporarily cannot access their account information, but systems were being brought back online Tuesday. The utility company provides power to 25,000 members and didn't pay a ransom after the attack. The company also did not have any compromised data resulting from the attack.

Member account information and payment systems were taken offline by maintenance as a precaution during the attack. The customers with prepaid accounts were not disconnected during the incident and won't be in the future. Some websites continue to have broken links, but information technicians are reestablishing customer sites. The attack was discovered last Saturday and does not seem to be connected to the Kaseya ransomware attack that has affected thousands of organizations in 17 countries.

(Source: OODA Loop)