U.S. Fire Administration | FEMA

EMR-ISAC InfoGram April 28 – Guidance on lithium-ion battery fires in electric bikes and scooters; Arson Awareness Week

EMR-ISAC sent this bulletin at 04/29/2022 12:08 PM EDT

View as a webpage / Share

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

The InfoGram

Volume 22 — Issue 17 | April 28, 2022

FDNY provides guidance on lithium-ion battery fires in electric bikes and scooters

Lithium-ion batteries are everywhere now. If your fire department has not yet experienced a fire involving a lithium-ion battery-powered device, it is only a matter of time before you do.

FirefighterCloseCalls.com recently highlighted the surge in lithium-ion battery fires from electric scooters and bikes in New York City.

E-bikes and electric scooters, also called “mobility devices,” are growing in popularity as a form of transportation in New York City and many other cities across the United States. New Yorkers commonly store and charge their mobility devices inside their homes, garages, or businesses. For this reason, many of these battery fires have led to structure fires, like the apartment fire in the Bronx that left 12 people injured in January of last year and seriously injured an FDNY firefighter.

Fires started by the batteries in mobility devices are becoming so frequent in New York City that the Fire Department of the City of New York (FDNY) issued a warning in October 2021, with tips to educate the public on how to charge, store, and use these batteries safely.

Nevertheless, these fires continue to happen frequently, and with serious consequences. Lithium-ion battery fires in mobility devices were responsible for four deaths in New York City in 2021, and just this month, the City saw four separate e-bike fires in two days, leaving a dozen injured.

Highlights

The FDNY has created several resources to educate the public and to teach firefighters how to safely extinguish these fires.

The first line of defense is prevention. FDNY Smart, a public education program within FDNY, has created a safety video on how to properly charge, use, and store consumer lithium-ion batteries.

For firefighters, the FDNY is providing best practices in its Tips from Training series:

- E-bikes and e-scooters fires/emergencies. This tip sheet provides tactical considerations for all aspects of response to these incidents, including personal protective equipment, hazardous materials response, safety procedures to protect from thermal runaway, and more.
- Revel e-bike battery transport vans. This tip sheet provides information on the vehicles that transport discharged lithium-ion batteries from rented mobility devices within the city. These vans contain as many as 60 batteries in a small, confined space, presenting significant hazards and extinguishment challenges.
- Lithium-ion battery mobility device fires. This tip sheet covers some of the same tactical considerations of the previous tip sheets, but also covers scene preservation prior to arrival of fire marshals and what to do after the fire has been knocked down.

These Tips from Training from FDNY could be used by many fire departments, especially in cities or large metropolitan areas where electrically powered mobility devices such as e-bikes and scooters are becoming more commonplace.

(Source: FirefighterCloseCalls.com)

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

Arson Awareness Week focuses on arson in homeless communities, webinar May 2

Every year during the first full week in May, the United States Fire Administration (USFA) observes Arson Awareness Week. During the week, USFA shares information to raise awareness about arson or youth firesetting and to provide strategies to combat these problems.

This year's theme is "Arson in Homeless Communities: Engagement – Education – Outreach."

Although arson incidents in the United States have trended steadily downward between 2010 and 2019, arson has been on the rise since 2019, according to the view of arson crime trends within the Federal Bureau of Investigation's (FBI's) Crime Data Explorer (CDE). The FBI's expanded crime data for 2020 reveals that of the 39,851 arson incidents in 2020, 37.8% of these involved structures (residential, commercial, industrial, storage, community/public, or other buildings).

With roughly 40% of arson fires occurring in structures, the presence of vacant buildings brings an

increased risk, and this risk is even greater in areas with both vacant buildings and vulnerable homeless populations.

The USFA has partnered with the National Volunteer Fire Council (NVFC) to host a webinar on **Monday, May 2, from 2-3 p.m. EST**. This webinar will feature presenters from the Indianapolis Fire Department's Fire Investigation Section, the Indianapolis Metropolitan Police Department, and Portland (Oregon) Fire and Rescue.

Presenters will provide information on arson as it relates to our nation's homeless population, using a holistic community risk reduction approach to address fire and life safety in this quickly growing risk area. Indianapolis' program will be featured, including strategies that have been implemented to combat the issue of vacant residence fires, the difficulties in effectively prosecuting these cases, the complex nature of the growing homeless problem, and how to identify resources and develop fire prevention programs within the homeless community

Those interested can learn more and register for the webinar via the USFA's website or the NVFC's website.

(Sources: USFA, NVFC, FBI)

FEMA's new Building Codes Strategy will foster resilient communities through modern building code adoption

At the 2022 National Hurricane Conference in Orlando, Florida this month, the Administrator of the Federal Emergency Management Agency (FEMA) announced the release of FEMA's new Building Codes Strategy and urged collective action to increase community adoption of modern, hazard-resistant building codes.

Disasters have a devastating impact on communities across the country. One of the most cost-effective ways to safeguard communities against natural disasters is to adopt and follow hazard-resistant building codes.

FEMA's landmark building codes study found that U.S. communities who chose to adopt modern building codes will avoid paying $132 billion in damages by the year 2040. However, 65% of the country's counties, cities and towns still have not adopted modern building codes and will not receive this benefit.

FEMA's new Building Codes Strategy organizes and prioritizes FEMA activities to advance the adoption and enforcement of hazard-resistant building codes and standards for FEMA programs. It promotes integrating building codes and standards across FEMA, strengthening nationwide capability and expertise for superior building performance, and driving public action to adopt and enforce building codes.

The new Strategy considers the role that building codes have on addressing the effects of climate change. It also acknowledges that low-income communities have been shown to be disproportionately impacted by natural hazards. Individuals in low-income communities are less likely to live in housing constructed according to modern building codes. FEMA plans to expand support to these communities to foster safe and resilient communities nationwide.

FEMA's Building Codes Executive Steering Group, supported by the Building Codes Work Group, developed the Building Codes Strategy over the course of two years. Visit FEMA's website to learn more about FEMA's new Building Codes Strategy and to view and download supporting documents.

(Source: FEMA)

Webinar: Update on National Address Database and Florida's NG911 PSAP training program

The National 911 Program will host a webinar in its State of 911 series on **Tuesday, May 10 at 12:00 p.m. EST**. The webinar will include an update on the National Address Database (NAD) and a discussion on Florida's statewide virtual NG911 Public Safety Answering Point (PSAP) training program

The first part of the webinar on the National Address Database will provide an overview of how the NAD has developed into a successful government undertaking without a mandate.

Accurate and up-to-date addresses are critical to transportation safety and are a vital part of Next Generation 911 (NG911). They are also essential for a broad range of government services, and the data can help enable critical applications, including public health tracking, natural disaster response, transportation planning, and more.

The webinar reviews the history of the NAD, from its beginnings in 2015 when the Department of Transportation began the National Address Database initiative—an aggregation of authoritative address points. Today, data is collected and maintained at the tribal or local government level and, in most cases, compiled at the state level before voluntary submission to the NAD.

The second part of the webinar will discuss Florida's statewide virtual NG911 PSAP training program. Given the shortage of in-person training opportunities during the pandemic, the Florida Department of Management Services recognized the need for additional training for public safety professionals concerning NG911 implementation. This discussion will focus on how the Florida Division of Telecommunications used grant funds to create a training program and virtual training workshops to educate on NG911 trends, standards and best practices while providing hands-on learning opportunities.

This webinar is free and open to everyone but advanced registration is required.

Visit the National 911 Program's website to learn more about the State of 911 webinar series, view past webinars, and sign up for email alerts.

(Source: National 911 Program)

Cyber Incident Assistance

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

IdentityTheft.gov

IC3

Cybercrime Support Network

General Information

StopRansomware.gov

CISA's Known Exploited Vulnerabilities Catalog

FTC scam list

CISA alerts

Law Enforcement Cyber Center

TLP Information

CISA, FBI, NSA, and international partners warn organizations of top routinely exploited cybersecurity vulnerabilities

The Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Federal Bureau of Investigation (FBI), Australian Cyber Security Centre (ACSC), Canadian Centre for Cyber Security (CCCS), New Zealand National Cyber Security Centre (NZ NCSC), and the United Kingdom's National Cyber Security Centre (NCSC-UK) issued a joint Cybersecurity Advisory on Wednesday, April 27 on the common vulnerabilities and exposures (CVEs) frequently exploited by malicious cyber actors, including the 15 most commonly exploited of 2021.

While the top 15 vulnerabilities have previously been made public, this Advisory is meant to help organizations prioritize their mitigation strategies. All organizations are encouraged to review and implement the recommended mitigations in this detailed joint CSA.

(Source: CISA)

CISA and FBI update advisory on Destructive Malware Targeting Organizations in Ukraine

CISA and the FBI have updated joint Cybersecurity Advisory AA22-057A: Destructive Malware Targeting Organizations in Ukraine, originally released February 26, 2022. The advisory has been updated to include additional indicators of compromise for WhisperGate and technical details for HermeticWiper, IsaacWiper, HermeticWizard, and CaddyWiper destructive malware. CISA and the FBI encourage organizations to review the update to AA22-057A as well as the Shields Up Technical Guidance webpage for ways to identify, respond to, and mitigate disruptive cyber activity.

(Source: CISA)

HHS: HC3 Analyst Note - Hive Ransomware

Hive is an exceptionally aggressive, financially-motivated ransomware group known to maintain sophisticated capabilities who have historically targeted healthcare organizations frequently. The Department of Health and Human Services (HHS) Health Sector Cybersecurity Coordination Center (HC3) recommends the Healthcare and Public Health (HPH) Sector be aware of their operations and apply appropriate cybersecurity principles and practices found in this document in defending their infrastructure and data against compromise

Read the full Analyst Note from HC3 on HHS' website.

(Source: HHS HC3)

Zero-day attacks surged in 2021, Mandiant says

Mandiant said that its intelligence division has documented a surge in verified zero-day exploits over the course of the last year, with 2021 accounting for 40% of zero-day attacks undertaken in the last decade. A zero-day vulnerability is a flaw in software or hardware which threat actors identify and exploit. Attackers then release malware before a developer can create a patch to address the vulnerability.

Mandiant Intelligence on Thursday identified 80 zero-days exploited "in the wild" — that is, in active use — in 2021, more than double the previous record volume set in 2019. Mandiant said it analyzed more than 200 zero-day vulnerabilities from 2012 to 2021.

(Source: CyberScoop)

AWS reissues Log4Shell hotpatch after vulnerabilities found

After the Log4j vulnerability was disclosed in early December, numerous vendors released patches to protect customers against potentially catastrophic cyber intrusions. Amazon Web Services (AWS) released a software tool in mid-December designed to patch vulnerabilities found in the Log4j library, however security researchers at Palo Alto's Unit 42 discovered code vulnerabilities that could let attackers break out of a container environment and gain escalated privileges.

After working with Palo Alto researchers for months, Amazon released a new hotpatch earlier this week, Unit 42 said in research released Tuesday. Unit 42 researchers urge organizations to review their container environments and upgrade to the fixed version. A large number of users may have downloaded the original hotpatches.

(Source: Cybersecurity Dive)

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