



The InfoGram

Volume 19 — Issue 10 | April 4, 2019

Dutch firefighters dunk \$155,000 smoking hybrid BMW in vat of water

After being called to a showroom for a smoking electric hybrid BMW i8, [firefighters in the Netherlands used a crane to immerse the car in a vat of water](#). The department stated they will keep the car submerged for 24 hours, just to be sure the fire is out. [This model of car sells for between \\$147,000 and \\$163,000](#).

While this response seems extreme at first, lithium battery systems used in hybrid electric vehicles are tricky to manage when they catch fire. Fire can spread easily from one battery to all the others connected to it, and fires can reignite repeatedly over days or weeks. It can take very large amounts of water to put out such a fire and it still may reignite.

While these fires are very rare, fire departments should ensure personnel are trained in both hybrid vehicle fire suppression and the safety hazards of such battery systems. [Tactics normally used for gasoline fires may make the situation worse](#). The vehicle must also be stored differently after the accident as a safeguard.

The National Fire Protection Association (NFPA) offers "[Alternative Fuel Vehicles Safety Training](#)" for the fire service, EMS, fire investigations, crash reconstruction, and tow and salvage companies. The self-paced, 4-hour training is free; students will receive a certificate upon completion.

NFPA also offers many other resources including [Emergency Response Guides from 30 alternative fuel vehicle manufacturers](#), free to download. At a minimum, be sure to watch the short "[Stranded Energy - How Little You Know Might Shock You](#)" video covering the basic but most important steps to take when encountering hybrid and electric cars involved in a traffic crash.

(Source: [NFPA](#))

Wildland Urban Interface Chief's Guide

Last year, federal [wildfire suppression costs topped \\$3 billion nationwide](#) (PDF, 70 Kb) for the first time, and fire losses for the major California wildfires alone are over \$9 billion. Life and property losses from wildfires continue to climb, and communities face greater risks every year.

Wildfires are a low-risk but high-impact event for most communities. According to the International Association of Fire Chief's (IAFC) [Wildland Urban Interface Chief's Guide](#), communities are now at risk that never were before due to factors such as urban creep and increased drought. Many of these jurisdictions have not adequately planned or prepared for such an event.

This IAFC guide walks fire chiefs and other officials through wildfire planning using the four phases of emergency management: preparedness, response, recovery and mitigation. Using case studies from all parts of the country, the guide details successful best practices already in use, giving fire departments new to wildfire planning a leg up and the ability to get started without having to reinvent the wheel.

IAFC hosts the file on its website in an interactive reader and as a downloadable 32.5 Mb PDF file.

(Source: [IAFC](#))

Highlights

Dutch firefighters dunk \$155,000 smoking hybrid BMW in vat of water

Wildland Urban Interface Chief's Guide

Upcoming GPS reset may affect operations

LockerGoga ransomware primer from the MS-ISAC



U.S. Fire Administration

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

Upcoming GPS reset may affect operations

On April 6, 2019, GPS will have a once in a 19.7 year event: the field used to track weeks will reset to zero.

Basically, GPS transmits a week number so your receiver can calculate the date. The week number is 10 bits long, which works out to 1094 weeks, or 19.7 years. This means every 19.7 years the number must reset to zero.

While GPS receivers built in accordance with industry standards should manage the event without incident, the Department of Homeland Security (DHS) encourages you to take steps to ensure your systems are ready:

- Check if any of your GPS receivers were built before 2010.
- If so, check with the manufacturer for firmware, hardware or software updates.

DHS encourages you to review how time is used in your organization and develop plans for managing your timing requirements. Below are two presentations providing a simplified overview of what the rollover is and steps you should take to prepare.

- The first document is [designed for business leaders to explain why managing timing requirements is important](#) (PDF, 709 Kb).
- The second document provides an [overview for businesses to follow to identify timing requirements and selecting appropriate timing source\(s\)](#) (PDF, 1 Mb).

[The Department of Homeland Security \(DHS\) issued the initial notice in April of 2018](#) (PDF, 212 Kb).

(Source: [CISA](#))

LockerGoga ransomware primer from the MS-ISAC

The Multi-State Information Sharing & Analysis Center (MS-ISAC) released a Security Primer on LockerGoga Ransomware—a type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid.

Ransomware can be devastating to individuals and organizations. The Cybersecurity and Infrastructure Security Agency (CISA) discourages individuals and organizations from paying the ransom, as this does not guarantee access will be restored.

CISA encourages users and administrators to review MS-ISAC's [White Paper: Security Primer – LockerGoga](#) and associated indicators of compromise, [CISA's Ransomware page](#), and the U.S. Government's [Interagency Joint Guidance](#) for further information and to implement the following best practices:

- Create system back-ups.
- Be wary of emails and attachments from unknown or unverified senders.
- Ensure that systems are updated with the latest patches.

(Source: [US-CERT](#))

The U.S. Fire Administration maintains 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 emr-isac@fema.dhs.gov.

Disclaimer of Endorsement: The EMR-ISAC does not endorse the organizations sponsoring linked websites, and does not endorse the views they express or the products/services they offer.

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.

DHS and the FBI encourage recipients of this document to report information concerning suspicious or criminal activity to the local [FBI office](#) and also the [State or Major Urban Area Fusion Center](#).

For information specifically affecting the private sector critical infrastructure contact the **National Infrastructure Coordinating Center** by phone at **202-282-9201**, or by email at **nicc@dhs.gov**.