



Homeland
Security

Daily Open Source Infrastructure Report

24 July 2015

Top Stories

- A director of security research at IOActive who recently hacked into the system of a 2015 Jeep Cherokee reported that the hack could be repeated on hundreds of thousands of Chrysler vehicles with Uconnect telematics systems. – *Computerworld* (See item [3](#))
- Fiat Chrysler Automobiles issued a recall July 22 for 144,416 model year 2011 – 2015 Dodge Journey and Fiat Freemont 2.4-liter vehicles in the U.S. due to an issue in which engine covers can be dislodged, posing a fire-risk. – *Autoblog* (See item [5](#))
- Highway 128 in Lake Berryessa, California was shut down while 525 firefighters worked to battle a 6,000-acre wildfire that threatened nearly 200 structures and prompted mandatory evacuations. – *KCRA 3 Sacramento* (See item [18](#))
- Hewlett Packard's Zero Day initiative released four new remote code execution zero day vulnerabilities in Microsoft Internet Explorer. – *The Register* (See item [20](#))

Fast Jump Menu

PRODUCTION INDUSTRIES

- [Energy](#)
- [Chemical](#)
- [Nuclear Reactors, Materials, and Waste](#)
- [Critical Manufacturing](#)
- [Defense Industrial Base](#)
- [Dams](#)

SUSTENANCE and HEALTH

- [Food and Agriculture](#)
- [Water and Wastewater Systems](#)
- [Healthcare and Public Health](#)

SERVICE INDUSTRIES

- [Financial Services](#)
- [Transportation Systems](#)
- [Information Technology](#)
- [Communications](#)
- [Commercial Facilities](#)

FEDERAL and STATE

- [Government Facilities](#)
- [Emergency Services](#)

Energy Sector

1. *July 23, Associated Press* – (West Virginia) **Regulators cite Murray Energy subsidiary for fatal accident.** A subsidiary of Murray Energy, McElroy Coal Co., was cited July 22 by the U.S. Mine Safety and Health Administration July for employing faulty mining methods and failing to adequately support the roof, face and wall, after a March 2015 incident where 1 miner died and 3 others injured after a piece of rock fell from an exposed area where a longwall machine was extracting coal.
Source: <http://www.wfmj.com/story/29614128/regulators-cite-murray-energy-subsidiary-for-fatal-accident>
2. *July 22, KHON 2 Honolulu* – (Hawaii) **Generator shutdown cuts power to 57,000 customers.** Hawaiian Electric Company officials reported that emergency outages were launched across Oahu July 22, leaving 57,000 without power after the island's largest generating unit shut down unexpectedly.
Source: <http://khon2.com/2015/07/22/no-additional-blackouts-expected-after-oahu-power-plant-goes-down/>

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

Critical Manufacturing Sector

3. *July 23, Computerworld* – (National) **Hacker: 'hundreds of thousands' of vehicles are at risk of attack.** A director of security research at IOActive who recently hacked into the system of a 2015 Jeep Cherokee from 10 miles away, reported that the hack could be repeated on hundreds of thousands of vulnerable model year 2013 – 2015 vehicles currently on the road, and that prior access to the vehicle is not required for a zero day-style attack, which works on any Chrysler vehicle with the Uconnect telematics system.
Source: http://www.networkworld.com/article/2951837/security/hacker-hundreds-of-thousands-of-vehicles-are-at-risk-of-attack.html#tk.rss_all
4. *July 22, U.S. Department of Labor* – (Georgia) **LaGrange, Georgia agriculture equipment manufacturer exposes workers to deadly safety hazards.** The Occupational Safety and Health Administration cited LaGrange-based Durand-Wayland Inc., July 22 with 11 serious and 10 other safety violations for issues including failure to identify permit-required confined spaces, failing to test air quality in confined spaces, and exposing workers to fall and welding hazards, among others. Proposed penalties total \$44,710.
Source: https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEA

[SES&p_id=28308](#)

5. *July 22, Autoblog* – (National) **Dodge Journey and Fiat Freemont engine-cover recall affects 350k CUVs.** Fiat Chrysler Automobiles issued a recall July 22 for 144,416 model year 2011 – 2015 Dodge Journey and Fiat Freemont 2.4-liter vehicles in the U.S. with 4-cylinder engines due to an issue in which engine covers can be dislodged, posing a fire-risk.
Source: <http://www.autoblog.com/2015/07/22/dodge-journey-fiat-freemont-engine-cover-recall/>

For another story, see item [21](#)

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

6. *July 22, Reuters* – (National) **Citi to shut Banamex USA, pay \$140 million fine.** Citigroup Inc., announced July 22 plans to liquidate subsidiary Banamex USA and pay \$140 million in fines to the Federal Deposit Insurance Corporation and California's Department of Business Oversight to resolve allegations that Banamex USA failed to comply with Federal anti-money laundering requirements and the Bank Secrecy Act.
Source: <http://www.reuters.com/article/2015/07/22/us-banamex-citigroup-idUSKCN0PW1Z520150722>
7. *July 22, KYTV 3 Springfield* – (Missouri) **Springfield restaurant owner and son plead guilty in multi-million dollar fraud scheme.** An owner of multiple Springfield area restaurants and commercial properties and his son pleaded guilty July 22 to charges that they submitted false financial documents to Great Southern Bank in order to receive 4 commercial loans worth about \$6 million in 2011.
Source: http://www.ky3.com/news/local/springfield-restaurant-owner-son-plead-guilty-in-multimillion-dollar-fraud-scheme/21048998_34299122

Transportation Systems Sector

8. *July 23, WRDW 12 Augusta* – (South Carolina) **All lanes of Edgefield Highway back open after accident.** All lanes of Edgefield Highway in Aiken County reopened July 23 after being closed overnight July 22 while crews responded to a 2-vehicle accident.
Source: <http://www.wrdw.com/home/headlines/Accident-with-injuries-closes-part-of-Edgefield-Hwy-318234471.html?ref=471>
9. *July 23, CNN* – (Wisconsin) **5 injured in plane crash at Wisconsin airshow.** A single-engine Piper Malibu crashed July 22 during the Experimental Aircraft Association's AirVenture airshow in Oshkosh, and injured 5 people. Both the U.S. Federal Aviation Administration and the National Transportation Safety Board were investigating the crash.

Source: <http://www.cnn.com/2015/07/22/us/wisconsin-plane-crash-air-show/>

10. *July 23, Associated Press* – (New York; Canada) **NY oil tank car inspections lead to 1 immediate fix.** New York officials reported that an investigation of 524 tank cars and 152 miles of tracks and 38 rail switches revealed 62 defects between Alberta, Canada and New York, including 1 where there was a missing bolt on a continuously welded rail joint which required an immediate fix.

Source: <http://www.beaumontenterprise.com/news/article/NY-oil-tank-car-inspections-lead-to-1-immediate-6401039.php>

11. *July 22, Associated Press* – (Washington) **WSP: 4 people killed in crash on Highway 2.** The Washington State Patrol reported that Highway 2 near Davenport in Lincoln County was shut down for several hours July 22 while crews responded to an accident after a vehicle crossed the center lane and hit a semi-truck head on, killing 4 people.

Source: <http://q13fox.com/2015/07/22/wsp-several-people-killed-in-crash-on-highway-2/>

For another story, see item [18](#)

Food and Agriculture Sector

Nothing to report

Water and Wastewater Systems Sector

12. *July 23, WHTH 27 Harrisburg* – (Pennsylvania) **Midstate state park beach closed over health concerns.** The Pennsylvania departments of Health and Conservation and Natural Resources shut down the beach at Cowans Gap State Park in Fulton County after 2 dozen cases were reported of people becoming sick after swimming in the lake July 18 – July 19, prompting an investigation.

Source: <http://abc27.com/2015/07/22/midstate-state-park-beach-closed-over-health-concerns/>

13. *July 22, Middletown Patch* – (Rhode Island) **Blue green algae found in Paradise Pond in Middletown.** The Rhode Island State Department of Health and Environmental Management issued an advisory that people should avoid contact with the water in Paradise Pond in Middletown until November due a blue-green algae bloom which produces toxins that are harmful to humans and animals. The town's water supply is not at risk.

Source: <http://patch.com/rhode-island/middletown/blue-green-algae-found-paradise-pond-middletown-0>

Healthcare and Public Health Sector

14. *July 22, ABC News* – (National) **Medicare funds totaling \$60 billion improperly paid, report finds.** The U.S. Government Accountability Office released a report July 22 which revealed 23,400 potentially fake or incorrect addresses on Medicare's list of

health care providers, causing an estimated \$60 billion lost to fraud, waste, abuse and improper payments under the Medicare system. Medicare responded to the findings stating that they do not have the authority to cross-check State and license revocation or suspension in states where a physician is not set up to bill Medicare.

Source: <http://abcnews.go.com/Politics/medicare-funds-totaling-60-billion-improperly-paid-report/story?id=32604330>

Government Facilities Sector

15. *July 23, USA Today* – (Montana) **Fire near Glacier National Park doubles in size.** Winds in Glacier National Park expanded wildfires that have been raging for the past several weeks to 4,000 acres, forcing the evacuation of campers in St. Mary Valley July 22 and destroying at least one historic structure in the park.
Source: <http://www.usatoday.com/story/news/nation/2015/07/23/fire-spreads-near-glacier-national-park/30548783/>
16. *July 23, Associated Press* – (Washington) **Hundreds fighting wildfire near Walla Walla; 1 home burned.** Sections of forest roads in the Umatilla National Forest were closed July 23 after a fire approached Mill Creek Watershed, which provides drinking water for 60,000 residents of Walla Walla. The cause of the fire is under investigation, although authorities say it was likely human-caused.
Source: <http://www.seattletimes.com/seattle-news/hundreds-fighting-wildfire-near-walla-walla-1-home-burned/>
17. *July 22, Alaska Dispatch News* – (Alaska) **City says contractor error caused phone, email outage at Anchorage City Hall.** Employees at Anchorage City Hall lost access to telephones, email, timekeeping, and the electronic financial system for several hours July 22 due to a network outage at the South Anchorage data center. The city's 9-1-1 system was not affected, and there was no lasting damage.
Source: <http://www.adn.com/article/20150722/city-says-contractor-error-caused-phone-email-outage-anchorage-city-hall>

Emergency Services Sector

18. *July 23, KCRA 3 Sacramento* – (California) **Lake Berryessa fire grows to 6,000 acres; mandatory evacuations issued.** Highway 128 in Lake Berryessa was shut down for an unspecified amount of time while a total of 525 firefighters worked to battle an explosive wildfire that grew to 6,000 acres overnight and threatened nearly 200 structures prompting mandatory evacuations. Officials believe the cause of the fire was a vehicle crash but the investigation is ongoing.
Source: <http://www.kcra.com/news/wildfire-prompts-evacuations-near-lake-berryessa/34303526>

Information Technology Sector

19. *July 23, Threatpost* – (International) **Four zero days disclosed in internet explorer.** Hewlett Packard's Zero Day Initiative released four new remote code execution (RCE)

zero day vulnerabilities in Microsoft's Internet Explorer, including an issue in how the browser processes arrays representing cells in Hypertext Markup Language (HTML) tables in which an attacker could execute code under the context of the current process. Source: <https://threatpost.com/four-zero-days-disclosed-in-internet-explorer/113911>

20. *July 23, The Register* – (International) **Flash zero-day monster Angler dominates exploit kit crime market.** Security researchers from SophosLabs reported that the Angler exploit kit's (EK) prevalence in the underground malware market has ballooned from about 25 – 83 percent between September 2014 and May 2015, likely due to factors including its low cost and high traffic to Angler-infected Web sites. The EK recently incorporated three Adobe Flash zero-day flaws that were exposed in the breach of Hacking Team. Source: http://www.theregister.co.uk/2015/07/23/sophos_angler_ek/

21. *July 23, The Register* – (International) **Cyber poltergeist threat discovered in Internet of Stuff hubs.** Security researchers from Tripwire's Vulnerability and Exposure Research Team (VERT) discovered vulnerabilities in Internet of Things-enabled smart home hubs made by Wink, Vera, and SmartThings, that could allow an attacker to obtain root shell access on the device, provide entry points to the home network. Source: http://www.theregister.co.uk/2015/07/23/home_hub_insecurity_iot_stalking/

22. *July 23, Help Net Security* – (International) **Smartwatches: a new open frontier for attack.** Hewlett Packard released findings from an assessment of 10 smart-watches and their Android and iOS cloud and mobile application components revealing that each watch contained significant vulnerabilities, including insufficient authentication, lack of encryption, insecure software, firmware, interfaces, and privacy concerns. Source: <http://www.net-security.org/secworld.php?id=18658>

23. *July 22, Threatpost* – (International) **Bartalex variants spotted dropping Pony, Dyre malware.** Security researchers at Rackspace reported that strains of the macro-based Bartalex malware has been observed dropping Pony loader malware along with the Dyre banking trojan. Source: <https://threatpost.com/bartalex-variants-spotted-dropping-pony-dyre-malware/113903>

For another story, see item [3](#)

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web site: <http://www.us-cert.gov>

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: <http://www.it-isac.org>

Communications Sector

24. *July 22, Athens Messenger* – (Ohio) **Phone service could be out for a while.** Frontier Communications reported July 22 that a telephone outage has occurred in the south side area of Athens to the Meigs County Line after a telephone cable was damaged during construction work on Richland Avenue. The extent of damage remains under assessment and a company spokesperson reported that it would take a couple of days for service to be fully restored.
Source: http://www.athensmessenger.com/news_briefs/phone-service-could-be-out-for-a-while/article_6abd5565-e376-519b-a651-bee0db5a67d2.html

For another story, see item [17](#)

Commercial Facilities Sector

25. *July 23, WRAL 5 Raleigh* – (North Carolina) **Two Raleigh police officers taken to hospital after hotel fire.** Two police officers and 3 civilians were injured and taken to an area hospital July 22 after a fire at a Raleigh Wake Inn was intentionally set in an apartment unit. Emergency crews responded to the incident and an investigation is ongoing.
Source: <http://www.wral.com/raleigh-motel-fire-sends-three-to-hospital/14789663/>
26. *July 23, KHOU 11 Houston* – (Texas) **3-alarm fire damages FM 1960 shopping center.** A 3-alarm fire heavily damaged the Harris County FM 1960 shopping center including Lasagna House restaurant and Barney's Saloon pool hall, and prompted 4 fire departments to respond to contain the incident. No injuries were reported.
Source: <http://www.khou.com/story/news/local/2015/07/23/fire-reported-at-fm-1960-shopping-center/30557093/>

For another story, see item [18](#)

Dams Sector

Nothing to report



Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for 10 days on the Department of Homeland Security Web site: <http://www.dhs.gov/IPDailyReport>

Contact Information

Content and Suggestions:	Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703) 942-8590
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes .
Removal from Distribution List:	Send mail to support@govdelivery.com .

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@hq.dhs.gov or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.