Daily Open Source Infrastructure Report
18 February 2016

Top Stories

- General Motors Corporation issued a recall February 16 for approximately 180,000 vehicles including Saab and Saturn Astra models due to potentially faulty Takata Corporation PSDI-5 driver front air bag inflators. – *Detroit Free Press* (See item **4**)
- PTC Inc., and 2 of its Chinese subsidiaries agreed to pay more than $28 million February 16 to settle parallel civil and criminal actions involving violations of the Foreign Corrupt Practices Act. – *U.S. Securities and Exchange Commission* (See item **5**)
- Officials closed a 24-mile stretch of Interstate 70 in Glenwood Springs, Colorado, through at least February 18 while crews worked to remove debris from a February 15 rockslide. – *Associated Press* (See item **7**)
- Rhode Island State Police announced that a teenager was arrested February 12 in connection to at least 15 bomb hoaxes at schools and businesses inside and outside of the State. – *WCVB 5 Boston; Associated Press* (See item **14**)

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. *February 16, WABC 7 New York City* – (New York; New Jersey) **Severe weather brings flooding, power outages, wind damage to Tri-State.** Heavy rain and strong winds February 16 delayed flights, flooded roadways, and caused over 50,000 customers in New Jersey and New York to lose power.
   Source: http://abc7ny.com/weather/severe-weather-brings-flooding-power-outages-wind-damage-/1203002/

2. *February 16, NJ.com* – (New Jersey) **1,500 gallons of oil spill in Elizabeth, authorities say.** Officials are investigating the cause of a 1,500 gallon oil spill near the Arthur Kill in Elizabeth, New Jersey, February 16 while crews worked to contain the oil.
   Source: http://www.nj.com/union/index.ssf/2016/02/1500-gallon_oil_spill_draws_union_county_hazmat_te.html

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

Critical Manufacturing Sector

3. *February 17, Softpedia* – (International) **Backdoor in MVPower DVR firmware sends CCTV stills to an email address in China.** Security researchers from Pen Test Partners discovered digital video recorder (DVR) devices manufactured by MVPower and deployed by closed-circuit television (CCTV) surveillance systems were vulnerable to security flaws which can allow attackers to execute Man-in-the-Middle (MitM) attacks, bypass the device's Web-based login system, and use a backdoor functionality to send CCTV feed snapshots to a hard-coded email address hosted on a Chinese email provider, among other vulnerabilities.
   Source: http://news.softpedia.com/news/backdoor-in-mvpower-dvr-firmware-sends-cctv-stills-to-an-email-address-in-china-500502.shtml

4. *February 16, Detroit Free Press* – (International) **GM recalls 200,000 Saabs, Saturns for air bag inflators.** General Motors Corporation issued a recall February 16 for approximately 180,000 vehicles including model years 2003 – 2011 Saab 9-3 vehicles, model years 2010 – 2011 Saab 9-5 vehicles, and model years 2008 – 2009 Saturn Astra vehicles sold in the U.S. due to potentially faulty Takata Corporation PSDI-5 driver front air bag inflators after 10 worldwide deaths and over 100 injuries were linked to the bags deploying improperly when activated and discharging metal fragments into vehicle occupants. Approximately 20,000 of the vehicles affected by the recall are located in Canada.
   Source: http://www.freep.com/story/money/cars/general-motors/2016/02/16/gm-recall-

saab-saturn-takata-air-bag/80444792/

For another story, see item **20**

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

5. *February 16, U.S. Securities and Exchange Commission* – (International) **SEC: Tech company bribed Chinese officials.** The U.S. Securities and Exchange Commission announced February 16 that Massachusetts-based PTC Inc., and 2 of its Chinese subsidiaries agreed to pay more than $28 million to settle parallel civil and criminal actions involving violations of the Foreign Corrupt Practices Act (FCPA) after the 2 subsidiaries provided nearly $1.5 million worth of improper travel, gifts, and entertainment to Chinese government officials from 2006 – 2011 in an effort to win business. The subsidiaries disguised the payments as legitimate business expenses and PTC Inc., failed to stop the illicit payments despite indicators of corruption.
Source: https://www.sec.gov/news/pressrelease/2016-29.html

Transportation Systems Sector

6. *February 17, LancasterOnline* – (Pennsylvania) **Police blame stop sign violation for truck crash that closed Route 30 near Paradise.** A 6-mile stretch of Lincoln Highway East in Paradise Township was closed for nearly 5 hours February 16 following a 2-vehicle crash that knocked down a utility pole.
Source: http://lancasteronline.com/news/local/lincoln-highway-east-closed-from-accident-with-live-wires-across/article_49d8de5c-d4e6-11e5-9b0a-8763f4f04cc8.html

7. *February 17, Associated Press* – (Colorado) **Rock slide forces closure of major Colorado highway.** Officials closed a 24-mile stretch of Interstate 70 in Glenwood Springs through at least February 18 while crews worked to remove debris from a February 15 rockslide.
Source: http://www.msn.com/en-us/news/us/rock-slide-forces-closure-of-major-colorado-highway/ar-BBpAtLl

8. *February 16, KQTV 2 Saint Joseph* – (Missouri) **One killed in US Hwy 59 crash.** U.S. Highway 59 in Buchanan County was closed for approximately 5 hours February 16 while crews worked to clear the wreckage from a fatal 2-vehicle crash involving a semi-truck that killed 1 driver.
Source: http://www.stjoechannel.com/news/local-news/crash-blocks-traffic-on-us-hwy-59

9. *February 15, WCTI 12 New Bern* – (North Carolina) **Both lanes of traffic now open on Hwy. 264 after accident scene cleared.** A 6-vehicle crash involving 2 semi-trucks and 4 other vehicles shut down eastbound and westbound lanes of Highway 264 in Pitt

County for several hours February 15 while crews worked to clear the wreckage.
Source: http://www.wcti12.com/news/highway-remains-closed-due-to-icy-crash-involving-6-vehicles/38000258

For another story, see item **1**

Food and Agriculture Sector

10. *February 17, Binghamton Press & Sun-Bulletin* – (New York) **Barn Fire: Rubble cleared after 71 cows lost.** Authorities are investigating the cause of a February 16 fire destroyed a barn in Afton and killed 71 cows that were trapped inside.
Source: http://www.pressconnects.com/story/news/public-safety/2016/02/16/fire-damages-afton-barn/80443774/

11. *February 17, U.S. Department of Agriculture* – (Pennsylvania) **Winter Gardens Quality Foods, Inc. recalls chicken salad products due to possible foreign matter contamination.** Winter Gardens Quality Foods, Inc., in New Oxford, Pennsylvania, issued a recall February 16 for approximately 3,710 pounds of its Southwest Chicken Salad products sold in 10-pound bulk tubs after the establishment's oil supplier notified the company of a packaging defect where plastic pieces could break off into the oil used in the product, causing potential plastic contamination. The items were shipped to a distributer in Pennsylvania for further processing and distribution.
Source: http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2016/recall-018-2016-release

12. *February 16, U.S. Food and Drug Administration* – (National) **Forever Cheese recalls imported Mitica brand Pecorino Aged Cheese in Walnut Leaves for possible health risk.** New York-based Forever Cheese Inc., issued a recall February 16 for 40 cases of its Pecorino Foglie di Noci products from 1 specific production code after routine sampling revealed that the cheese tested positive for Listeria monocytogenes. The company is investigating the cause of the contamination which affected products shipped to retail locations and restaurants in nine States.
Source: http://www.fda.gov/Safety/Recalls/ucm486414.htm

Water and Wastewater Systems Sector

Nothing to report

Healthcare and Public Health Sector

13. *February 16, Palm Beach Post* – (Florida) **PBSO: Teen arrested for pretending to be doctor in West Palm Beach.** Authorities arrested a man February 16 who was allegedly pretending to be a doctor and practicing medicine without a license out of the New Birth New Life Holistic and Alternative Medical Center & Urgent Care in West Palm Beach following an undercover investigation.
Source: http://www.palmbeachpost.com/news/news/crime-law/pbso-teen-pretended-to-be-doctor-in-west-palm/nqQ9H/

Government Facilities Sector

14. *February 17, WCVB 5 Boston; Associated Press* – (Rhode Island) **Rhode Island teenager arrested for series of bomb hoaxes at schools and businesses.** State police in Rhode Island announced that a student from Rogers High School in Newport was arrested February 12 in connection to at least 15 bomb hoaxes at schools and businesses inside and outside of the State. Officials stated that the teenager was running the calls through a Russian Web site to avoid detection.
Source: http://www.wcvb.com/news/rhode-island-teenager-arrested-for-series-of-bomb-hoaxes-at-schools-and-businesses/38037714

15. *February 17, Hawaii News Now* – (Hawaii) **Shelters opened for residents displaced by Kahikinui brush fire.** Crews worked to contain a 5,500-acre brush fire February 17 burning in Kahikinui, Maui, which has prompted the displacement of several residents.
Source: http://www.hawaiinewsnow.com/story/31239431/shelters-opened-for-residents-displaced-by-kahikinui-brush-fire

16. *February 16, Easton Express-Times* – (Pennsylvania) **Burst sprinkler pipe causes heavy damage at Forks Elementary.** Classes at Forks Elementary School in Pennsylvania were cancelled February 16 – February 17 after a broken sprinkler pipe caused extensive damage to several classrooms February 14 and destroyed workbooks and textbooks. Crews worked to clean up the damages.
Source:
http://www.lehighvalleylive.com/easton/index.ssf/2016/02/burst_sprinkler_pipe_causes_he.html

17. *February 16, Brockton Enterprise* – (Massachusetts) **Massasoit cancels Wednesday classes at Brockton due to power outage.** Classes at Massasoit Community College in Brockton were cancelled February 17 following a power outage February 15 caused by a faulty switch gear. Utility crews worked to locate the issue and restore service.
Source: http://www.wickedlocal.com/article/20160216/NEWS/160217168

Emergency Services Sector

See item **20**

Information Technology Sector

18. *February 17, SecurityWeek* – (International) **Fysbis backdoor preferred by Pawn Storm group to target Linux.** Security researchers at Palo Alto Networks released a report revealing that the Pawn Storm threat group improved their obfuscation technique for their preferred Linux malware, Fysbis, to ensure that the malware installation information is no longer available in the open and that the malware runs a series of shell commands to establish persistency through newly found command and control (C&C) domain mozilla-plugins[.]com, which was reportedly believed to be associated to a newer campaign.

Source: http://www.securityweek.com/fysbis-backdoor-preferred-pawn-storm-group-target-linux

19. *February 16, Softpedia* – (International) **Buffer overflow bug in glibc exposes users to attacks from rogue DNS servers.** Security researchers from Google's Project Zero and Red Hat fixed a security flaw in GNU C Library (glibc) that could allow an attacker to send oversized Domain Name System (DNS) responses and force buffer overflow and remote code execution attacks, enabling hackers to run malicious code on a victim's machine with the same privileges as glibc's parent application. Google released a proof-of-concept code that should help system administrators detect if their systems are vulnerable to the flaw.
Source: http://news.softpedia.com/news/buffer-overflow-bug-in-glibc-exposes-users-to-attack-from-rogue-dns-servers-500484.shtml

20. *February 16, SecurityWeek* – (International) **Unpatched flaw plagues Cisco industrial switches.** Cisco reported February 15 that IOS software 15.2(4)E running on its Industrial Ethernet 2000 Series Switches is vulnerable to a denial-of-service (DoS) issue due to the faulty way its system processes Cisco Discovery Protocol (CDP) packets which could allow an unauthenticated attacker to send specially crafted CDP packets. In addition, Cisco reported that its Emergency Responder product was vulnerable to a cross-site scripting (XSS) flaw, which can allow an unauthenticated attacker to execute arbitrary code in the context of the vulnerable Web interface and access potentially sensitive browser information.
Source: http://www.securityweek.com/unpatched-flaw-plagues-cisco-industrial-switches

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

Nothing to report

Commercial Facilities Sector

21. *February 16, Milford Daily News* – (Massachusetts) **Bellingham: Flooding causes apartment evacuation again.** The Jefferson at Bellingham apartment complex in Massachusetts was evacuated out of an abundance of caution February 15 due to a flooding incident caused by a ruptured pipe. All displaced residents were given short-term housing and local fire and building officials worked to identify the cause of the incident.

Source: http://www.milforddailynews.com/article/20160216/NEWS/160216827

For another story, see item **14**

Dams Sector

Nothing to report

NTAS
National Terrorism Advisory System
NO ACTIVE ALERTS
www.DHS.gov/alerts

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.