# Daily Open Source Infrastructure Report
# 03 October 2016

## Top Stories

- Och-Ziff Capital Management Group agreed to pay $200 million September 29 to settle charges that the firm's executives used intermediaries and business partners to pay bribes to high-level government officials in Africa in order to secure mining rights. – *U.S. Securities and Exchange Commission* (See item **4**)
- The Baltimore City Department of Public Works reported September 29 that more than 10,000 gallons of sewage and rainwater flowed into the Jones Falls following severe rainstorms in the area that began September 28. – *WBFF 45 Baltimore* (See item **18**)
- The Texas Water Development Board awarded a $5.4 million loan to the City of Edinburg, Texas September 22 to complete the expansion of the city's West Water Treatment Plant. – *Edinburg Review* (See item **19**)
- The Marin Healthcare District and Prima Medical Foundation announced September 28 that more than 5,000 patients medical data was lost due to a glitch in their system following a July ransomware attack. – *Marin Independent Journal* (See item **20**)

---

**Fast Jump Menu**



---

## Energy Sector

1. *September 29, Allentown Morning Call* – (Pennsylvania) **Bethlehem gas leak closes streets, prompts evacuations.** A gas leak, sinkhole, and water line break in Bethlehem, Pennsylvania, prompted officials to evacuate a 3-block radius around North New Street, condemn 3 homes, and cut power to 4,000 PPL Electric Utilities customers for several hours September 29. The causes of the leaks remain under investigation.
   Source: http://www.mcall.com/news/breaking/mc-gas-leak-reported-in-bethlehem-evacuations-underway-20160929-story.html

For additional stories, see items **4** and **25**

## Chemical Industry Sector

Nothing to report

## Nuclear Reactors, Materials, and Waste Sector

Nothing to report

## Critical Manufacturing Sector

2. *September 30, SecurityWeek* – (International) **Cisco forgets to remove testing interface from security appliance.** Cisco inadvertently introduced a critical vulnerability in both its physical and virtual Email Security Appliances (ESA) running IronPort and AsyncOS software that could allow a remote attacker to gain control of the affected device with root privileges due to an internal testing and debugging interface that attacks can connect to without authorization. Cisco advised users to reboot their devices using the reboot command from the command-line interface in order to disable the internal testing and debugging interface.
   Source: http://www.securityweek.com/cisco-forgets-remove-testing-interface-security-appliance

3. *September 28, U.S. Department of Labor* – (Texas) **OSHA fines Houston machinery rebuilder more than $155K for continuing to expose workers to amputation, other hazards.** The Occupational Safety and Health Administration cited Machinery Maintenance Rebuilders Inc. with 1 serious and 1 failure to abate citation September 28 after an August 2016 follow-up inspection at the Houston facility revealed that the company exposed workers to amputation hazards, failed to properly secure hazardous machinery, and failed to install energy-control devices on machinery. Proposed penalties total $155,139.
   Source:
   https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=33225

## Defense Industrial Base Sector

Nothing to report

## Financial Services Sector

4. *September 29, U.S. Securities and Exchange Commission* – (International) **Och-Ziff executives also settle charges.** The U.S. Securities and Exchange Commission (SEC) announced September 29 that Och-Ziff Capital Management Group agreed to pay roughly $200 million to settle charges that the firm's executives disregarded red flags and corruption risks as determined by the Foreign Corrupt Practices Act (FCPA), and used intermediaries, agents, and business partners to pay bribes to high-level government officials in Africa in order to secure mining rights and corruptly influence government officials in 5 African countries. SEC officials stated that Och-Ziff fraudulently documented the bribe payments and neglected to maintain proper internal controls to recognize or prevent the bribes.
   Source: https://www.sec.gov/news/pressrelease/2016-203.html

5. *September 29, SecurityWeek* – (International) **Dridex banking trojan adopts improved encryption.** MalwareTech security researchers discovered the Dridex banking trojan started using malicious Rich Text Format (RTF) files that are password protected in order to prevent automated systems from scanning the attachment for malicious code and to avoid detection. Researchers also found Dridex employs delayed execution and may be focused on infecting corporate systems.
   Source: http://www.securityweek.com/dridex-banking-trojan-adopts-improved-encryption

6. *September 28, U.S. Department of Justice* – (International) **Dual Jamaican-U.S. citizen pleads guilty in connection with Jamaica-based lottery fraud scheme.** A dual Jamaican and U.S. citizen pleaded guilty September 28 for her role in a Jamaica-based fraudulent lottery scheme where she persuaded U.S. citizens to send her hundreds of thousands of dollars to cover fraudulent fees for lottery winnings that victims had not won and never obtained, causing U.S. citizens tens of millions of dollars in losses from 2011 – 2012. The charges state the dual citizen used some of the funds for personal expenses.
   Source: https://www.justice.gov/opa/pr/dual-jamaican-us-citizen-pleads-guilty-connection-jamaica-based-lottery-fraud-scheme

## Transportation Systems Sector

7. *September 30, Hagerstown Herald-Mail* – (Maryland) **Traffic reopened on eastbound I-70 near Hancock.** Eastbound lanes of Interstate 70 near Hancock, Maryland, were closed for more than 9 hours September 30 while crews worked to remove the wreckage following 2 separate accidents. Both collisions remain under investigation.
   Source: http://www.heraldmailmedia.com/news/breaking/eastbound-i--closed-in-hancock-due-to-fatal-accident/article_a27ff824-86f7-11e6-adcb-337ba07b280d.html

8. *September 30, Pittsburgh Post-Gazette* – (Pennsylvania) **Driver of tractor-trailer killed along I-79 in Franklin Park.** Interstate 79 in Franklin Park, Pennsylvania, was reduced to 1 lane in both directions, and a portion of Rochester Road was closed for several hours September 30 while officials investigated the scene after a semi-truck crashed into an overpass, killing the driver.
Source: http://www.post-gazette.com/local/north/2016/09/30/Driver-of-tractor-trailer-killed-along-I-79-in-Franklin-Park-pittsburgh/stories/201609300248

9. *September 29, Florida Today* – (Florida) **Southbound I-95 reopens near Wickham Road.** Southbound lanes of Interstate 95 near Wickham Road in Viera, Florida, were closed for more than 3 hours September 29 while crews worked to clear the wreckage after a semi-truck crashed and spilled fuel on the roadway.
Source: http://www.floridatoday.com/story/news/local/2016/09/29/sb--95-shut-down-near-wickham-road/91286566/

10. *September 29, KLAS 8 Las Vegas* – (Nevada) **US 95 was closed from Flamingo to Boulder Hwy. most of Thursday, fleeing suspect hit by semi-truck.** Northbound lanes of U.S. 95 in Las Vegas were closed for about 3 hours September 29, while southbound lanes remained closed for about 9 hours following a 2-vehicle crash involving a semi-truck and another vehicle that was fleeing from police.
Source: http://www.lasvegasnow.com/news/us-95-closed-from-flamingo-to-boulder-highway

11. *September 29, KLFY 10 Lafayette* – (Louisiana) **I-10 now open in both directions following hazmat leak between Duson and Scott.** Interstate 10 between Duson and Scott, Louisiana, was closed for several hours September 29 while HAZMAT crews worked to remove a semi-truck that was leaking molten sulfur on the roadway. Officials advised residents to avoid the area.
Source: http://klfy.com/2016/09/29/i-10-east-and-west-closed-between-duson-and-scott-due-to-18-wheeler-leaking-hazardous-materials/

## Food and Agriculture Sector

12. *September 30, U.S. Food and Drug Administration* – (National) **Fresh Express announces precautionary recall of a limited quantity of 11 oz. American Salad due to possible allergen exposure.** Fresh Express Inc. issued a precautionary voluntary recall September 29 for 480 cases of its Fresh Express American Salad products sold in 11-ounce packages due to undeclared egg, milk, wheat, and anchovy after a small number of Caesar Salad condiment packets that contain the undeclared allergens were inadvertently included in the products. No illnesses have been reported and the products were distributed to retail establishments in six States.
Source: http://www.fda.gov/Safety/Recalls/ucm523266.htm

13. *September 30, KGPE 47 Fresno* – (California) **Massive fire burns Tos Farm in Hanford.** A September 29 fire at Tos Farms Inc. near Hanford, California, destroyed a building where walnuts are harvested and caused up to $6 million in damage. No

injuries were reported and the cause of the fire remains under investigation.
Source: http://www.yourcentralvalley.com/news/massive-fire-burns-tos-farm-in-hanford

14. *September 29, WSPY 107.1 FM Plano* – (Illinois) **3000 bushels of corn lost in Hinckley farm fire.** A September 28 fire at Herrmann Farms in Hinckley, Illinois, destroyed 3,000 bushels of corn after a corn dryer ignited. No injuries were reported.
Source: http://www.wspynews.com/news/local/bushels-of-corn-lost-in-hinckley-farm-fire/article_e7d016b2-8660-11e6-a825-ef236256efd0.html

15. *September 29, WBIW 1340 AM Bedford* – (Indiana) **Fire causes $550,000 in damages to Martin County turkey farm.** A September 27 fire at Pleasant View Turkey Farm near Whitfield, Indiana, killed approximately 10,000 turkeys and destroyed 2 turkey barns. No injuries to people were reported and authorities stated the fire began when burning cardboard was pulled through the farm's ventilation system.
Source: http://www.wbiw.com/local/archive/2016/09/fire-causes-550000-in-damages-to-martin-county-turkey-farm.php

16. *September 28, KERO 23 Bakersfield* – (California) **Izumo Sushi shut down by the Kern County Department of Public Health after cockroach infestation.** Izumo Sushi in Bakersfield, California, was shut down until further notice September 27 while health officials investigate after finding cockroaches at the restaurant.
Source: http://www.turnto23.com/news/local-news/izumo-sushi-shut-down-by-the-kern-county-department-of-public-health-after-cockroach-infestation

## Water and Wastewater Systems Sector

17. *September 30, Florida Today* – (Florida) **Melbourne boil-water alert mostly rescinded.** City officials in Melbourne, Florida, lifted a precautionary boil water advisory September 30 for all areas except the Tampa Avenue area in Indialantic and Spinnaker Point Court in Indian Harbour Beach after tests showed the water was safe to drink following a September 27 storm that knocked water pumps offline at the John A. Buckley Water Treatment Plant. The boil water restrictions were also lifted for all Brevard Public Schools ancillary sites and schools.
Source: http://www.floridatoday.com/story/news/2016/09/29/boil-water-advisory-expected-end-friday/91284934/

18. *September 29, WBFF 45 Baltimore* – (Maryland) **At least 10,000 gallons of sewage, rainwater released into Jones Falls: DPW.** The Baltimore City Department of Public Works reported September 29 that more than 10,000 gallons of sewage and rainwater flowed into the Jones Falls following severe rainstorms in the area that began September 28. City officials advised the public to avoid contact with urban streams.
Source: http://foxbaltimore.com/news/local/at-least-10000-gallons-of-sewer-water-released-into-jones-falls-dpw

19. *September 29, Edinburg Review* – (Texas) **Edinburg awarded $5.4 million to finish water treatment plant upgrade.** The Texas Water Development Board awarded a

$5.4 million loan to the City of Edinburg, Texas September 22 through the agency's Drinking Water State Revolving Fund to complete the expansion of the city's West Water Treatment Plant. The expansion includes adding 2 raw water pumps, 2 contact reactor clarifiers, and a 2 million gallon ground storage tank, among other improvements.
Source: http://www.edinburgreview.com/news/20160929/edinburg-awarded-54-million-to-finish-water-treatment-plant-upgrade

## Healthcare and Public Health Sector

20. *September 30, Marin Independent Journal* – (California) **Marin patients' medical data lost after cyber attack.** The Marin Healthcare District and Prima Medical Foundation announced September 28 they are notifying more than 5,000 patients that their medical data, including limited clinical history, vital signs, and documentation of physical examinations, among other information, was lost due to a glitch in Marin Medical Practice Concepts' system following a ransomware attack in July. Officials stated patients' personal, financial, and health information was not accessed, viewed, or transferred.
Source: http://www.marinij.com/article/NO/20160929/NEWS/160929766

## Government Facilities Sector

21. *September 30, WSLS 10 Roanoke* – (Virginia; West Virginia) **School delays, road closures and power outages.** Pocahontas County Schools in West Virginia were closed September 30 due to flood warnings and heavy rain in the region, which knocked out power to more than 500 Appalachian Power customers in Bedford and Botetourt counties in Virginia.
Source: http://wsls.com/2016/09/30/school-delays-road-closures-and-power-outages/

22. *September 29, KGO 7 San Francisco* – (California) **Firefighter injured battling massive Loma Fire in Santa Cruz Mountains.** Over 1,000 crews reached 34 percent containment September 29 of the 4,147-acre Loma Fire burning in the Santa Cruz Mountains in California, which has destroyed 8 homes, 9 other structures, and threatens at least 300 more. Officials lifted evacuation orders for all Santa Cruz County residents September 28, while road closures and evacuation orders for Santa Clara County remain in effect.
Source: http://abc7news.com/news/firefighter-injured-battling-massive-loma-fire/1532749/

For another story, see item **17**

## Emergency Services Sector

Nothing to report

## Information Technology Sector

23. *September 30, SecurityWeek* – (International) **Tofsee malware distribution switched from exploit kit to spam.** Security researchers from Cisco Talos reported that attackers stopped distributing the Tofsee ransomware via the RIG exploit kit (EK), and began leveraging spam email campaigns to deliver the malware downloaders, which instruct victims to download and open the ZIP archive attached to the message that contains an obfuscated JavaScript file with a WScript downloader, which runs an executable from a remote server controlled by the attacker. Researchers stated the malware allows hackers to conduct cryptocurrency mining, carry out distributed denial-of-service (DDoS) attacks, and send spam, among other malicious actions.
Source: http://www.securityweek.com/tofsee-malware-distribution-switched-exploit-kit-spam

For another story, see item 2

**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

See item 2

## Commercial Facilities Sector

24. *September 29, WJBK 2 Detroit* – (Michigan) **Firefighters battle 4-alarm blaze at commercial building in Grosse Point.** Authorities are investigating the cause of a 4-alarm fire at the Jim Saros Real Estate Agency in Grosse Pointe, Michigan, September 29. No injuries were reported.
Source: http://www.fox2detroit.com/news/local-news/208757350-story

25. *September 29, Modesto Bee* – (California) **Car crashes into gas meter, forces evacuation at apartments.** The El Casa Verde apartments in Modesto, California, were evacuated for around 3 hours September 29 after a vehicle crashed into a gas meter, causing a large gas leak. Firefighters and Pacific Gas and Electric Company crews shut off the gas.
Source: http://www.modbee.com/news/article104978566.html

## Dams Sector

26. *September 29, WNCN 17 Goldsboro* – (North Carolina) **As flood waters rise, NC dams threaten to give way.** Federal officials reported September 29 that the Long Valley Farm Lake Dam at Carvers Creek State Park in North Carolina had a partial

breach, and Rhodes Pond Dam near Godwin and the McLaughlin Lake Dam in Hoke County failed following heavy rains and flooding in the area.
Source: http://wncn.com/2016/09/29/as-flood-waters-rise-nc-dams-threaten-to-give-way/


## 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