Security updates for Monday

Ransomware: Claim that 22% SMBs shutting shop after attacks

Ransomware attacks caused 22% of small and medium-sized businesses in seven countries, including Australia, to pack up for good, a report from the security firm Malwarebytes claims.

Swedish Cabinet reshuffled in wake of IT security row

It’s not often that an IT security breach leads to the departure of two government ministers. But that is just what has happened in Sweden in the aftermath of a series of disclosures about a data breach and an outsourced IT contract.

Active Management of Open Source Components Delivers Measurable Improvements Claims Sonatype Report
In July, Sonatype released their third annual State of the Software Supply Chain report concluding that when organisations actively manage the quality of open source components in software applications they see a 28% improvement in developer productivity (through reduction in manual governance), a 30% reduction in overall development costs, and a 48% increase in application quality (as application vulnerabilities are removed early reducing their incidence in production). Analysis also showed that applications built by teams utilising automated governance tools reduced the percentage of defective components by 63%.

- **The CIA?s Aeris Malware Can Exfiltrate Data From Linux Systems** [6]

  Not a week goes by without WikiLeaks unveiling some more condemning evidence of the CIA?s malware tools. The latest reveal is Aeris, an automated implement which affects many different distributions of the Linux operating system. This particular tool packs quite a lot of features under the hood in an effort to gather as much intelligence as possible. This is surely not the last tool of its kind we will meet.

- **Firejail A Namespace Separation Security Sandbox** [7]

  Linux distro is mostly loved for its security features. When we people want more security we use TOR and VPN. Today I am going to tell you about an application called Firejail that helps to protect your personal files via sandbox technique.

  Firejail is a sandbox application built for Linux distros which uses the capabilities of Linux kernel to use namespace separation. In the simplest sense, apps launched through Firejail cannot access your personal files on your hard drive. Isn?t that cool? Cool and safe!

- **Defcon vote-hacking village shows that "secure" voting machines can be broken in minutes** [8]

  Nearly 20 years later, the country's voting security debt has mounted to incredible heights, and finally, just maybe, the security researchers are getting the hearing they deserve.

- **Def Con hackers showed how easily voting machines can be hacked** [9] [Ed: Windows powered] [10]

  At Def Con's hacker voting machine village, where 30 pieces of election equipment sat waiting, hackers were given a deliciously wicked goal. John Hopkins computer scientist Matt
Blaze said, "We encourage you to do stuff that if you did on election day they would probably arrest you."

And they did. Most of the voting machines were purchased via eBay, but some did come from government auctions. Despite the various different manufacturers of the voting equipment boxes, there was a common theme—they are "horribly insecure."

Granted, come election day, officials would likely notice if hackers were physically taking apart the machines. Tinkering with an external USB port on a computerized voting box and using it to upload malicious software may or may not get noticed. Yet those are not the only ways hackers could potentially influence votes and an election's outcome; there's the sneaky way of remotely accessing the machine from a laptop.

- **How DEF CON Securely Streams Video to Hackers** [11] [Author: "Linux Powered!"]

  The DEF CON 25 security conference is famous for its wide variety and number of security sessions and events. Not everyone can be in every session and some even choose to watch remotely, which is where DEF CON TV (DCTV) comes into play.

  DCTV streamed several sessions from the event, both to local hotels as well as the outside internet. Securely setting up and managing the DCTV streaming is no easy task, but it's one that DEF CON hackers put together rapidly.

- **Windows 10 default user profile is potentially writable by everyone** [12]

  Microsoft refuses to fix the issue properly because there is a "simple command everyone can execute" but has not (to my knowledge) told anyone about this command because everyone assumes the issue has been fixed by KB4022715 and KB4022725

- **[Older] The Internet of Things : A disaster for no good reason** [13]

  The reason I'm frustrated is because if these things were designed this way, I would WANT them. I really wish my washing machine would tell me when the wash is done because I am EXTREMELY bad at remembering to go check on it. But I can't buy that, I can't buy something that just has a $5 microprocessor with just enough intelligence to connect to the internet and send me an email or a push notification if the buzzer on the washer goes off. The
only thing I can buy is a washing machine that's had a horrible, unreliable PC full of quarter-baked software crammed into it which will stop working when some godforsaken cloud service is "sunset", and which is so dependant on the reliability and trustworthiness of the software on the computer that if someone hacks it or the software has a bug, the washer can start spraying water at me when I have the loading door open.

- **'Most dangerous' banking trojan gets update** [14]

  Svpeng, designed to steal banking information through different means, now embeds itself in Android's accessibility services ? the software that helps users with disabilities navigate devices and apps, the cybersecurity firm said. So Svpeng is now able to steal any data in a text box and log all keystrokes.

- **Enterprise Network Monitoring Needs Could Hamper the Adoption of TLS 1.3** [15]

  The upcoming version of the Transport Layer Security (TLS) protocol promises to be a game changer for web encryption. It will deliver increased performance, better security and less complexity. Yet many website operators could shun it for years to come.

  TLS version 1.3 is in the final stages of development and is expected to become a standard soon. Some browsers, including Google Chrome and Mozilla Firefox, already support this new version of the protocol on an opt-in basis and Cloudflare enables it by default for all websites that use its content delivery network.

---

**Security**

**Source URL:** [http://www.tuxmachines.org/node/103495](http://www.tuxmachines.org/node/103495)

**Links:**
[1] [http://www.tuxmachines.org/taxonomy/term/59](http://www.tuxmachines.org/taxonomy/term/59)
[2] [https://lwn.net/Articles/729357/rss](https://lwn.net/Articles/729357/rss)
[10] [http://techrights.org/2015/06/06/voting-systems/](http://techrights.org/2015/06/06/voting-systems/)