Security Leftovers

By *Roy Schestowitz*
Created *11/06/2019 - 1:07pm*
Submitted by Roy Schestowitz on Tuesday 11th of June 2019 01:07:35 PM Filed under Security [1]

- **Report: Response to the Consultation on the Government's regulatory proposals regarding consumer Internet of Things (IoT) security [2]**

  Open Rights Group (ORG) is a UK-based digital campaigning organisation working to protect fundamental rights to privacy and free speech online. With over 3,000 active supporters, we are a grassroots organisation with local groups across the UK.

  We are a project partner to Values and Ethics in Responsible Technology in Europe (VIRT-EU) ? a European project funded by the Horizon 2020 program. VIRT-EU?s mission is to foster ethical thinking in IoT development. The following comments stem predominantly from our experience accumulated in the course of that project.

  We address the consultation questions in order below, omitting questions 7, 8 and 9 as these lie outside our remit.

  1. Do you agree that the Government should take powers to regulate on the security of consumer IoT products? If yes, do you agree with the proposed legislative approach?

  We welcome the proposal to create primary legislation to introduce enhanced security for consumers using IoT devices. We also support the approach of making some requirements mandatory in the first instance with a longer strategy.

- **'This Is a Bombshell': Facial Recognition Data Collected by US Customs Agency Hacked [3]**

  "This is a bombshell," said Evan Greer, deputy director of the advocacy group Fight fight for the Future, in response to the reporting. "Even if you 100% trust the US government with your biometric information (which you shouldn't) this is a reminder that once your face is scanned

and stored in a database, it's easily shared across government agencies, stolen by hackers, other governments, etc."

Buzzfeed, also among the first to report on the breach on Monday, noted that the "cyberattack comes amid the ongoing rollout of CBP's "biometric entry-exit system," the government initiative to biometrically verify the identities of all travelers crossing US borders." As BuzzFeed News reported Citing earlier reporting, Buzzfeed pointed out that "CBP is scrambling to implement the initiative with the goal of using facial recognition technology on '100 percent of all international passengers,' including American citizens, in the top 20 US airports by 2021."

- **What you need to know about the MDS vulnerability and Red Hat Virtualization [4]**

  A new series of vulnerabilities in Intel processors, known as Microarchitectural Data Sampling, or more simply MDS, was recently made public and Red Hat released information about how the vulnerabilities affect our software and how to protect your organization.

  In the simplest terms, MDS is a vulnerability in Intel processors similar to Spectre and Meltdown; it allows a guest to read protected memory from anywhere on the host or guest. To mitigate the risks exposed by MDS, a combination of updated microcode, updated kernel(s), patches, and administrator action will need to be taken for both the hypervisors and virtual machines in your Red Hat Virtualization deployment. Unlike some similar vulnerabilities, simply disabling SMT and/or hyper-threading is not enough to protect your applications.

- **5 reasons chaos engineering is indispensable to the CISO [5]**

  Security leaders, including the chief information security officer (CISO), are challenged to continuously demonstrate their role within the company's value stream as part of improving security. In doing so, a growing number of security organizations are shifting toward a more "applied security mode," leading many to rethink our traditional practices and question their effectiveness in today's high-velocity, software-driven world.

- **Wireless Security | Roadmap to Securing Your Infrastructure [6]**

- **IPFire on AWS: Update to IPFire 2.23 - Core Update 132 [7]**

  Today, we have updated IPFire on AWS to IPFire 2.23 - Core Update 132 - the latest official release of IPFire.

This update brings you the new Intrusion Prevention System out-of-the-box as well as updates to the whole system.

- **Amitabh Bachchan?s Twitter Account ?Hacked? And DP Got Changed** **[8]**

Security

Source URL: http://www.tuxmachines.org/node/124757

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] https://www.openrightsgroup.org/about/reports/response-to-the-consultation-on-the-governments-regulatory-proposals-regarding-consumer-internet-of-things-(iot)-security
[3] https://www.commondreams.org/news/2019/06/10/bombshell-facial-recognition-data-collected-us-customs-agency-hacked
[4] https://www.redhat.com/en/blog/what-you-need-know-about-mds-vulnerability-and-red-hat-virtualization
[5] https://opensource.com/article/19/5/reasons-chaos-engineering-ciso
[6] https://wpengine.linuxacademy.com/security/wireless-security-roadmap-to-securing-your-infrastructure/
[7] https://blog.ipfire.org/post/ipfire-on-aws-update-to-ipfire-2-23-core-update-132
[8] https://fossbytes.com/amitabh-bachchans-twitter-account-hacked-and-dp-got-changed/