

# Security Leftovers

By *Roy Schestowitz*

Created *15/10/2021 - 11:38pm*

Submitted by Roy Schestowitz on Friday 15th of October 2021 11:38:06 PM Filed under [Security](#) [1]

- [Security updates for Friday](#) [2]

Security updates have been issued by Debian (squashfs-tools, tomcat9, and wordpress), Fedora (openssh), openSUSE (kernel, mbedtls, and rpm), Oracle (httpd, kernel, and kernel-container), SUSE (firefox, kernel, and rpm), and Ubuntu (linux-azure, linux-azure-5.4).

- [Apache Releases Security Advisory for Tomcat?? | CISA](#) [3]

The Apache Software Foundation has released a security advisory to address a vulnerability in multiple versions of Tomcat. An attacker could exploit this vulnerability to cause a denial of service condition.

- [Security Risks of Client-Side Scanning](#) [4]

Even before Apple made their announcement, law enforcement shifted their battle for back doors to client-side scanning. The idea is that they wouldn't touch the cryptography, but instead eavesdrop on communications and systems before encryption or after decryption. It's not a cryptographic back door, but it still a back door ? and brings with it all the insecurities of a back door.

I'm part of a group of cryptographers that has just published a paper discussing the security risks of such a system. (It's substantially the same group that wrote a similar paper about key escrow in 1997, and other ?exceptional access? proposals in 2015. We seem to have to do this

every decade or so.) In our paper, we examine both the efficacy of such a system and its potential security failures, and conclude that it's a really bad idea.

- 

**[The Open Source Security Foundation receives \\$ 10 million in funding - itsfoss.net](https://www.itsfoss.net/the-open-source-security-foundation-receives-10-million-in-funding/)**[5]

The Linux Foundation has announced a \$ 10 million commitment to the OpenSSF (Open Source Security Foundation), an effort to improve the security of open source software. Funds raised through royalties from parent companies of OpenSSF, including Amazon, Cisco, Dell Technologies, Ericsson, Facebook, Fidelity, GitHub, Google, IBM, Intel, JPMorgan Chase, Microsoft, Morgan Stanley, Oracle, Red Hat, Snyk, and VMware ?

## [Security](#)

---

**Source URL:** <http://www.tuxmachines.org/node/156839>

**Links:**

[1] <http://www.tuxmachines.org/taxonomy/term/59>

[2] <https://lwn.net/Articles/873056/rss>

[3] <https://us-cert.cisa.gov/ncas/current-activity/2021/10/15/apache-releases-security-advisory-tomcat>

[4] <https://www.schneier.com/blog/archives/2021/10/security-risks-of-client-side-scanning.html>

[5] <https://www.itsfoss.net/the-open-source-security-foundation-receives-10-million-in-funding/>