1500 - Abusing Certificate Transparency Logs

Friday at 15:00 in Track 4

45 minutes | Demo, Tool

Hanno Böck*Hacker and freelance journalist*

The Certificate Transparency system provides public logs of TLS certificates. While Certificate Transparency is primarily used to uncover security issues in certificates, its data is also valuable for other use cases. The talk will present a novel way of exploiting common web applications like Wordpress, Joomla or Typo3 with the help of Certificate Transparency.

Certificate Transparency has helped uncover various incidents in the past where certificate authorities have violated rules. It is probably one of the most important security improvements that has ever happened in the certificate authority ecosystem. In September 2017 Google will make Certificate Transparency mandatory for all new certificates. So it's a good time to see how it could be abused by the bad guys.

Hanno Böck

Hanno Böck is a hacker and freelance journalist. He regularly covers IT security issues for the German IT news site Golem.de and publishes the monthly Bulletproof TLS Newsletter. He also runs the Fuzzing Project, an effort to improve the security of free and open source software supported by the Linux Foundation's Core Infrastructure Initiative.

@hanno

#defcon25/by_track/track4/Friday   #defcon25/By_Day/_Friday