Bad RSA Library Leaves Millions of Keys Vulnerable

Originalartikel

Backup

<html> So, erm… good news everyone! A vulnerability has been found in a software library responsible for generating RSA key pairs used in hardware chips manufactured by Infineon Technologies AG. The vulnerability, dubbed ROCA, allows for an attacker, via a Coppersmith’s attack, to compute the private key starting with nothing more than the public key, which pretty much defeats the purpose of asymmetric encryption altogether. Affected hardware includes cryptographic smart cards, security tokens, and other secure hardware chips produced by Infineon Technologies AG. The library with the vulnerability is also integrated in authentication, signature, and encryption tokens of other vendors and chips used for Trusted Boot of operating systems. Major vendors including Microsoft, Google, HP, Lenovo, and Fujitsu already released software updates and guidelines for mitigation. The researchers found and analysed vulnerable keys in various domains including electronic citizen documents (750,000 Estonian identity cards), authentication tokens, trusted boot devices, software package signing, TLS/HTTPS keys and PGP. The currently confirmed number of vulnerable keys found is about 760,000 but could be up to two to three orders of magnitude higher. Devices dating back to at least 2012 are affected, despite being NIST FIPS 140-2 and CC EAL 5+ certified.. The vulnerable chips were not necessarily sold directly by Infineon Technologies AG, as the chips can be embedded inside devices of other manufacturers. <blockquote> The difficulty of the factorization attack is not the same for all key lengths and is NOT strictly increasing (some longer keys may take less time to factorize than other shorter ones). The following key length ranges are now considered practically factorizable (time complexity between hours to 1000 CPU years at maximum): 512 to 704 bits, 992 to 1216 bits and 1984 to 2144 bits. Note that 4096-bit RSA key is not practically factorizable now, but may become so, if the attack is improved. The time complexity and cost for the selected key lengths (Intel E5-2650 v3@3GHz Q2/2014): <ul class=„fix-media-list-overlap“><li class=„level1“> 512 bit RSA keys – 2 CPU hours (the cost of $0.06); <li class=„level1“> 1024 bit RSA keys – 97 CPU days (the cost of $40-$80); <li class=„level1“> 2048 bit RSA keys – 140.8 CPU years, (the cost of $20,000 – $40,000). </blockquote> Keep in mind that these benchmarks are for a single CPU. For certain three-letter agencies one must assume the attacks take trivial time to complete. Then again, they probably already have your keys (citation needed). Concerned users can test their public keys online or, maybe a better idea, offline by cloning the following GitHub repository. If using Linux flavors with pip, you can try the following to test your known public keys: <pre class=„brush: bash; title: ; notranslate“ title=„“>

 $ sudo pip install roca-detect

 $ gpg -a –export > /tmp/public && roca-detect /tmp/public
 2017-10-17 14:10:33 [7869] INFO ### SUMMARY ####################
 2017-10-17 14:10:33 [7869] INFO Records tested: 93
 2017-10-17 14:10:33 [7869] INFO .. PEM certs: . . . 0
 2017-10-17 14:10:33 [7869] INFO .. DER certs: . . . 0
 2017-10-17 14:10:33 [7869] INFO .. RSA key files: . 0
 2017-10-17 14:10:33 [7869] INFO .. PGP master keys: 1
 2017-10-17 14:10:33 [7869] INFO .. PGP total keys: 102
 2017-10-17 14:10:33 [7869] INFO .. SSH keys: . . . 0
 2017-10-17 14:10:33 [7869] INFO .. APK keys: . . . 0
 2017-10-17 14:10:33 [7869] INFO .. JSON keys: . . . 0
 2017-10-17 14:10:33 [7869] INFO .. LDIFF certs: . .

0
 2017-10-17 14:10:33 [7869] INFO .. JKS certs: . . . 0
 2017-10-17 14:10:33 [7869] INFO .. PKCS7: 0
 2017-10-17 14:10:33 [7869] INFO No fingerprinted keys found (OK)
 2017-10-17 14:10:33 [7869] INFO ##############################

 </pre> In this example, no vulnerable keys were found. Did you find one? If it is yours, it’s probably better to revoke and generate a new one. It seems 2017 keeps on giving us security pearls with each passing day. Yesterday we mourned the death of WPA2, but we’ve also seen SHA-1 broken, the Broadcom WiFi exploit in one billion smartphones (Broadpwn), a Bluetooth vuln that won’t be patched in around 40% of the devices, your credentials being cached in search engines, and we left several from this list. </html>