Micha? Górny (Gentoo) and Daniel Kahn Gillmor (Debian) on OpenPGP Security

By *Roy Schestowitz*
Created *05/07/2019 - 3:02am*
Submitted by Roy Schestowitz on Friday 5th of July 2019 03:02:55 AM Filed under GNU [1] Linux [2] Gentoo [3] Security [4] Debian [5]

- **Micha? Górny: SKS poisoning, keys.openpgp.org / Hagrid and other non-solutions [6]**

  The recent key poisoning attack on SKS keyservers shook the world of OpenPGP. While this isn?t a new problem, it has not been exploited on this scale before. The attackers have proved how easy it is to poison commonly used keys on the keyservers and effectively render GnuPG unusably slow. A renewed discussion on improving keyservers has started as a result. It also forced Gentoo to employ countermeasures. You can read more on them in the ?Impact of SKS keyserver poisoning on Gentoo? news item.

Coicidentally, the attack happened shortly after the launch of keys.openpgp.org, that advertises itself as both poisoning-resistant and GDPR-friendly keyserver. Naturally, many users see it as the ultimate solution to the issues with SKS. I?m afraid I have to disagree ? in my opinion, this keyserver does not solve any problems, it merely cripples OpenPGP in order to avoid being affected by them, and harms its security in the process.

In this article, I?d like to shortly explain what the problem is, and which of the different solutions proposed so far to it (e.g. on gnupg-users mailing list) make sense, and which make things even worse. Naturally, I will also cover the new Hagrid keyserver as one of the glorified non-solutions.

- **Daniel Kahn Gillmor: WKD for debian.org [7]**

  By default, this will show you any matching certificate that you already have in your GnuPG local keyring. But if you don't have a matching certificate already, it will fall back to using WKD.

  These certificates are extracted from the debian keyring and published at https://openpgpkey.debian.org/.well-known/debian.org/, as defined in the WKD spec. We intend to keep them up-to-date when ever the keyring-maint team publishes a new batch of certificates. Our tooling uses some repeated invocations of gpg to extract and build the published tree of files.

  Debian is current not implementing the Web Key Directory Update Protocol (and we have no plans to do so). If you are a Debian developer and you want your OpenPGP certificate updated in WKD, please follow the normal procedures for Debian keyring maintenance like you always have.

GNU Linux Gentoo Security Debian

Source URL: http://www.tuxmachines.org/node/125555

Links:
[1] http://www.tuxmachines.org/taxonomy/term/144
[2] http://www.tuxmachines.org/taxonomy/term/63
[3] http://www.tuxmachines.org/taxonomy/term/109
[4] http://www.tuxmachines.org/taxonomy/term/59
[5] http://www.tuxmachines.org/taxonomy/term/141
[6] https://blogs.gentoo.org/mgorny/2019/07/04/sks-poisoning-keys-openpgp-org-hagrid-and-other-non-solutions/
[7] https://dkg.fifthhorseman.net/blog/wkd-for-debian.org.html