Security: WireGuard, SafeBreach and More

By *Roy Schestowitz*
Created *13/10/2019 - 7:18pm*
Submitted by Roy Schestowitz on Sunday 13th of October 2019 07:18:59 PM Filed under Security [1]

- **WireGuard Snapshot `0.0.20191012` Available** [2]

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256
Hello,
A new snapshot, `0.0.20191012`, has been tagged in the git repository.
Please note that this snapshot is a snapshot rather than a final
release that is considered secure and bug-free. WireGuard is generally
thought to be fairly stable, and most likely will not crash your
computer (though it may).  However, as this is a snapshot, it comes
with no guarantees; it is not applicable for CVEs.
With all that said, if you'd like to test this snapshot out, there are
few relevant changes.
== Changes ==
  * qemu: bump default version
  * netns: add test for failing 5.3 FIB changes

  Kernels 5.3.0 - 5.3.3 crash (and are probably exploitable) via this c

  unshare -rUn sh -c 'ip link add dummy1 type dummy && ip link set dumm

  We fixed this upstream here:

  https://git.kernel.org/pub/scm/linux/kernel/git/davem/net.git/commit/

  This is relevant to WireGuard because a very similar sequence of comm
  used by wg-quick(8).

  So, we've now added some tests to catch this code path in the future.
  the bug here was a random old use-after-free, the test checks the ger
```

```
  policy routing setup used by wg-quick(8), so that we make sure this c
  to work with future kernels.

  * noise: recompare stamps after taking write lock

  We now recompare counters while holding a write lock.

  * netlink: allow preventing creation of new peers when updating

  This is a small enhancement for wg-dynamic, so that we can update pee
  without readding them if they've already been removed.

  * wg-quick: android: use Binder for setting DNS on Android 10

  wg-quick(8) for Android now supports Android 10 (Q). We'll be releasi
  version of the app for this later today.
This snapshot contains commits from: Jason A. Donenfeld and Nicolas Dou
As always, the source is available at https://git.zx2c4.com/WireGuard/
information about the project is available at https://www.wireguard.com
This snapshot is available in compressed tarball form here:
  https://git.zx2c4.com/WireGuard/snapshot/WireGuard-0.0.20191012.tar.x
  SHA2-256: 93573193c9c1c22fde31eb1729ad428ca39da77a603a3d81561a9816cce
  BLAKE2b-256: d7979c453201b9fb6b1ad12092515b27ea6899397637a34f46e74b52
A PGP signature of that file decompressed is available here:
  https://git.zx2c4.com/WireGuard/snapshot/WireGuard-0.0.20191012.tar.a
  Signing key: AB9942E6D4A4CFC3412620A749FC7012A5DE03AE
If you're a snapshot package maintainer, please bump your package versi
you're a user, the WireGuard team welcomes any and all feedback on this
snapshot.
Finally, WireGuard development thrives on donations. By popular demand,
have a webpage for this: https://www.wireguard.com/donations/
Thank you,
Jason Donenfeld
```

- **WireGuard 0.0.20191012 Released With Latest Fixes [3]**

  WireGuard is still working on transitioning to the Linux kernel's existing crypto API as a faster approach to finally make it into the mainline kernel, but for those using the out-of-tree WireGuard secure VPN tunnel support, a new development release is available.

- **SafeBreach catches vulnerability in controversial HP Touchpoint Analytics software [4]**

  Now the feature is embroiled in another minor controversy after security researchers at SafeBreach said they uncovered a new vulnerability. HP Touchpoint Analytics comes

preinstalled on many HP devices that run Windows. Every version below 4.1.4.2827 is affected by what SafeBreach found.

In a blog post, SafeBreach Labs security researcher Peleg Hadar said that because the service is executed as "NT AUTHORITY\SYSTEM," it is afforded extremely powerful permissions that give it wide access.

"The CVE-2019-6333 vulnerability gives attackers the ability to load and execute malicious payloads using a signed service. This ability might be abused by an attacker for different purposes such as execution and evasion, for example: Application Whitelisting Bypass Signature Validation Bypassing," Hadar wrote.

[...]

The company has long had to defend HP Touchpoint Analytics against critics who say it gives HP unnecessary access to users' systems. When it first became widely noticed in 2017, dozens of users complained that they had not consented to adding the system.

- **Security Tool Sprawl Reaches Tipping Point** **[5]**

- **How trusted digital certificates complement open source security** **[6]**

  Application developers incorporating open source software into their designs may only discover later that elements of this software have left them (and their customers) exposed to cyber-attacks.

- **Securing the Container Supply Chain** **[7]**

Security

Source URL: http://www.tuxmachines.org/node/129242

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] https://lists.zx2c4.com/pipermail/wireguard/2019-October/004594.html
[3] https://www.phoronix.com/scan.php?page=news_item&px=WireGuard-20191012
[4] https://www.techrepublic.com/article/safebreach-catches-vulnerability-in-controversial-hp-touchpoint-analytics-software/
[5] https://www.darkreading.com/threat-intelligence/security-tool-sprawl-reaches-tipping-point/d/d-id/1336048
[6] https://www.scmagazineuk.com/trusted-digital-certificates-complement-open-source-security/article/1596283
[7] https://www.devprojournal.com/technology-trends/open-source/securing-the-container-supply-chain/