Re: [scr1101806] in-path attacks against VPNs

From <cve-request@mitre.org>
To <william@breakpointingbad.com>
Cc <cve-request@mitre.org>
Date 2021-07-05 14:22

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

Thank you for contacting us. We realize that you have completed
important work about previously unpublished threats that affect a
significant fraction of all VPN users. Our current thoughts are:

1. CVE-2019-14899 should not have been assigned. It is not valid
to have a CVE ID that is supposed to apply to a collection of
independently developed code that happens to be susceptible to the
same attack methodologies. For further information, please see
https://cve.mitre.org/cve/cna/rules.html section 7.2.4b.

2. To obtain a CVE ID, you would need to identify a single affected
codebase, and indicate what portion of the code has an implementation
mistake (accompanied, if possible, by the agreement of the software
maintainer on how the code has been, or could be, patched).

It looks like you might be able to do this for WireGuard, but we are
not certain of that. In your
https://www.usenix.org/system/files/sec21fall-tolley.pdf document,
statements such as

  "There is no operating system implementation detail, VPN
   design decision, or configuration setting that we can point to
   as being the vulnerability that enables our server-side attacks."

and

  "Our server-side attacks are not associated with any vulnerability;
   instead, they only assume that the VPN server correctly performs
   network address translation."

and

  "For server-side attacks there is not a concept of a vulnerable
   VPN technology or OS, because the attack takes advantage
   of NAT when working as specified."

suggest that a CVE ID is not applicable to any of the findings
related to server-side attacks. CVE IDs are assigned to software
mistakes; they are not assigned to attack methodologies.

3. More generally, we do not assign CVE IDs to research that is
ultimately a suggestion for a design improvement. Otherwise we
would, for example, enumerate every possible design improvement
in Tor, such as on the
https://www.torproject.org/docs/faq.html.en#AnonymityAndSecurity
page, and assign CVE IDs to them.

We do understand that there is an important distinction between your
research and the various research into attacks against Tor. VPNs are
more widely used than Tor, and some readers legitimately feel that
your research implies a conclusion of "the level of data security
provided by a VPN is often much worse than what the user is
expecting." Unfortunately, decisions about CVE ID assignment cannot be
influenced by an assessment of the importance of the research itself.

[Suggested description]
A vulnerability affecting Linux, FreeBSD, OpenBSD, macOS, iOS,
Android, and Windows that allows an in-path router to infer and hijack
TCP connections and DNS queries that are tunneled through OpenVPN,
WireGuard, or StrongSwan.

[Additional Information]
Artifact included with Usenix paper submission which contains demos, PCAPs, and a virtual environment to test the vulnerability:
https://git.breakpointingbad.com/Breakpointing-Bad-Public/vpn-attacks

---

[VulnerabilityType Other]
CWE-300: Channel Accessible by Non-Endpoint

[Vendor of Product]
OpenVPN, WireGuard, StrongSwan, Linux

[Affected Product Code Base]
OpenVPN, WireGuard, StrongSwan, Linux - All

[Attack Type]
Remote

[Impact Code execution]
true

[Impact Denial of Service]
true

[Impact Information Disclosure]
true

[Attack Vectors]
Any in-path router between the VPN client and VPN server sends packets to the VPN server spoofed from end-point (website or server the VPN user is connected to)

[Reference]
https://www.usenix.org/system/files/sec21fall-tolley.pdf
https://seclists.org/oss-sec/2020/q3/116
https://breakpointingbad.com/2020/08/12/VPN-FAQ.html

[Has vendor confirmed or acknowledged the vulnerability?]
true

[Discoverer]
Breakpointing Bad - William J. Tolley, Beau Kujath, and Jedidiah R. Crandall

- --
CVE Assignment Team
M/S M300, 202 Burlington Road, Bedford, MA 01730 USA
[A PGP key is available for encrypted communications at
  https://cve.mitre.org/cve/request_id.html]
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1

iQIcBAEBCAAGBQJg400vAAoJEPNX0OmQPkAIzsMP/jpu/mVZ1GSNSDhZ37o8o8Gq
NZtMrISYfBS9gKzla5nEO6kROV1hvrtJXzCYiKJ1H4VmSJx8O6yjmouww/3dMmQu
kXzKvbZw5wAFeRQp4MD+GMcfIN2+jdG8zf8l9V8ihcZVNBJsJmUTw6f9zeHDgCRk
GjEBMv5lHU+S6klUvxaprTU6Jx4uE0DWqebHxxhIKW/xYz4IjH4TxJGL2zI02Y8b
dOjLyk2dtq5Hssv0b13FrZjDe4zAny29akDAb3aOHY9BETXWD8gXmm2r/ZQ8ysbh
ukrp0Tvw0rA5uR0OzeWujiQuXWR8rUKHH31UdAG24QqDA7EJTQKmATm1M7Xc503n
G4ISyZH8jDwxLlWZPux+/ImUqFGoF/Gbvd5T9emiM5xw/ecyM+ZM1CBgI0pbl7L9
KdSUWfiUd5gLSyvqvttd5TWZZdbJFyHZtSAG9GzCMKTR7gl/kuMYJ0kBwiQqu7nF
o0Hfsi3zof2P9/UzMWVZW0TfkjRf9Ff6P5QyMaFiVT8gp1zs/DtbUJsTWi7W/M1d
fwnwHmUqKdz1DmBN82UdoY/CaYX737jHBe10Eu/cVBmWbQz4usMCFNLMm/Mlv4TM
JmnmUv9cKbWwBakgGDJs2EPEpDVzPbgv6kBFOQw5XCIGYp9bJHSMs3iQmOShsMdp
Yah+Nv8lfofMRmihwl6v
=a+wX
-----END PGP SIGNATURE-----