Report: No-Log VPNs Exposed Users' Logs and Personal Details for All to See

A group of free VPN (virtual private network) apps left their server completely open and accessible, exposing private user data for anyone to see. This lack of basic security measures in an essential part of a cybersecurity product is not just shocking. It also shows a total disregard for standard VPN practices that put their users at risk.

The vpnMentor research team, led by Noam Rotem, uncovered the server and found **Personally Identifiable Information (PII) data for potentially over 20 million VPN users,** according to claims of user numbers made by the VPNs.

Each of these VPNs claims that their services are "no-log" VPNs, which means that they don't record any user activity on their respective apps. However, **we found multiple instances of internet activity logs** on their shared server. This was in addition to the PII data, which included **email addresses, clear text passwords, IP addresses, home addresses,** phone models, device ID, and other technical details.

The VPNs affected are UFO VPN, FAST VPN, Free VPN, Super VPN, Flash VPN, Secure VPN, and Rabbit VPN – all of which appear to be connected by a common app developer and white-labeled for other companies.

Data Breach Summary

Apps	UFO VPN, FAST VPN, Free VPN, Super VPN, Flash VPN, Secure VPN, Rabbit VPN
Headquarters/Location	Hong Kong
Industry	Cybersecurity
Total size of data	1.207 TB
Total number of files	1,083,997,361 records
No. of people exposed	Over 20 million, based on user numbers claimed by the VPNs
Geographical scope	Worldwide
Types of data exposed	Activity logs, PII (names, emails, home address), cleartext passwords, Bitcoin payment information, support messages, personal device information, tech specs, account info, direct Paypal API links
Potential impact	Fraud, doxing, blackmail, extortion, viral attack, and hacking, arrest, and persecution
Data storage format	ElasticSearch Server

Company Profile

We believe **the VPNs exposed in this leak share the same developer,** based on the following findings:

- The VPNs share a common Elasticsearch server
- They are hosted on the same assets
- They have a single recipient for payments, Dreamfii HK Limited
- At least three of the VPNs on the server share almost identical branding on their websites

Super VPN

Home Privacy Policy Terms of Service

Best VPN solution for Android

- Unblock the world freely and easily
- Reclaim your right to privacy
- Enjoy the open Internet

Download on the App Store

GET IT ON Google Play

Download

Flash VPN

Home Privacy Policy Terms of Service

Best VPN solution for Android

- Unblock the world freely and easily
- Reclaim your right to privacy
- Enjoy the open Internet

GET IT ON Google Play

Download on the App Store

Download

Free VPN

Home Privacy Policy Terms of Service

Best VPN solution for Android

- Unblock the world freely and easily
- Reclaim your right to privacy
- Enjoy the open Internet

GET IT ON Google Play

Download on the App Store

Download

We believe that the VPNs are ‘white-labeled’ apps, **created by one entity and rebranded for use under multiple names.**

The brands the VPNs are marketed under include:

- **UFO VPN** – “Super private & unlimited fast VPN for Android. Hide IP, unblock sites from 360.”
  Google Play Store: Rating 4.5 stars, 10M+ downloads
  Apple App Store: 4.8 stars
  Developer: Dreamfii HK Limited, Hong Kong
- **FAST VPN** – “100% Free VPN for gaming: access websites, apps and mobile games unlimited”
  Google Play Store: Rating 4.5 stars, 1M+ downloads
  Apple App Store: Rating 4.6 stars
  Developer: Mobipotato HK Limited, Hong Kong
- **FREE VPN** – “The best free VPN tunnel for android to unblock content. Feel the outer space!”
  Google Play Store: Rating 4.5 stars, 100k+ downloads
  Apple App Store: Rating 4.6 stars
  Developer: Starxmobi HK Ltd, Hong Kong
- **Super VPN** – “Super VPN is the best unlimited VPN proxy for android.”
  Google Play Store: 4.6 stars, 1M+ downloads
  Apple App Store: 4.9 stars
  Developer: Nownetmobi, Hong Kong

Dreamfii, the listed developer of UFO VPN, advertises as a marketing company for businesses. Included on the same assets are the VPNs mentioned above, Flash VPN, Secure VPN for iOS, and more.

View by Hosting

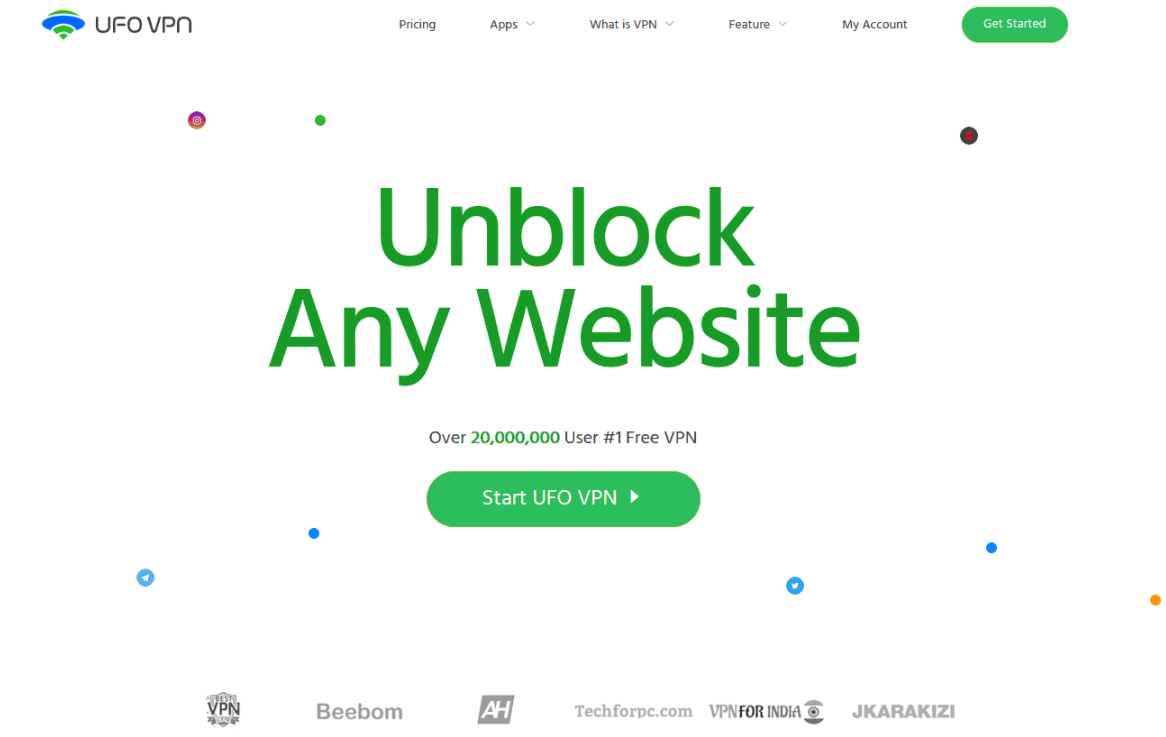
1 - 32 of 32 res

#	Domain	Alexa Rank	Hosting Provider	Mail Provider
1	blog-ufovpn-783813245.us-east-1.elb.amazonaws.com	-	Amazon.com, Inc.	-
2	www.bestvpn.im	-	Amazon.com, Inc.	-
3	bestvpn.im	-	Amazon.com, Inc.	-
4	fast-vpn.io	-	Amazon.com, Inc.	-
5	www.fast-vpn.io	-	Amazon.com, Inc.	-
6	www.fastvpn.im	-	Amazon.com, Inc.	-
7	www.flashvpn.net	-	Amazon.com, Inc.	-
8	flashvpn.net	-	Amazon.com, Inc.	China Unicom Shenzen network
9	www.free-vpn.io	-	Amazon.com, Inc.	-
10	free-vpn.io	-	Amazon.com, Inc.	China Unicom Shenzen network
11	maskvpn.im	-	Amazon.com, Inc.	-
12	www.maskvpn.im	-	Amazon.com, Inc.	-
13	blog.rabbitvpn.net	-	Amazon.com, Inc.	-

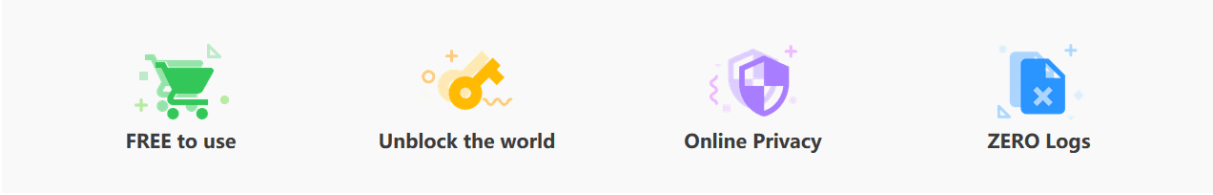
A screenshot from securitytrails.com showing the different domains hosted on a single IP address managed by the company that owns the VPN apps

According to their respective websites, every VPN provides military-grade security features and zero logs policies to reinforce their users' information security. However, this is contrary to what we found during our research.

We viewed detailed activity logs from each VPN, exposing users' personal information and browsing activities while using the VPNs and unencrypted plain text passwords, which are rarely used in military-grade security products.



UFO VPN states that they are the #1 free VPN and boasts over 20 million users



Many of the VPNs claim their apps are 'zero logs', including Free-vpn.io, pictured above

Strict ZERO Logs.
We do not store your original IP address. We do not log how you use FAST VPN connection. We do not sell, use, or disclose any personal data. You are safe with FAST VPN.

Fast VPN's 'Strict Zero Logs'affirmation

Security and Confidentiality

We use industry-standard information, security tools, and measures, as well as internal procedures and strict guidelines to prevent information misuse and data leakage. Our employees are subject to confidentiality obligations. We use measures and procedures that substantially reduce the risks of data misuse, but we cannot guarantee that our systems will be absolutely safe. If you become aware of any potential data breach or security vulnerability, you are requested to contact us immediately. We will use all measures to investigate the incident, including preventive measures, as required.

UFO VPN's security and confidentiality promise

3. Information We Collect and Store

* Personal information: The Service barely records your personal information except your geographic at the city level (please note that additional information may be collected if you contact us).
* Non-personal information: (i) Data related to your device information and, app version, connection time stamp, the server and the protocol you connected, total data used, network type and the error report (if any) will be automatically collected when you visit or use the Service. (ii) Analysis of our servers, which is non-identifying, like the analysis of the sites visited through the Service. This is a mixed big data form all our users.

Fast VPN's Privacy Policy

Timeline of Discovery and Owner Reaction

- **Date discovered:** July 5, 2020
- **Date VPNs notified:** July 5, 2020
- **Date VPNs contacted:** 5th to 14th July 2020
- **Date of Contact with HK CERT:** 8th July 2020
- **Date server was closed:** 15th July 2020

Sometimes, the extent of a data breach and the owner of the data are obvious, and the issue quickly resolved. But rare are these times. Most often, we need days of thorough investigation before we understand what's at stake or who's exposing the data.

Understanding a breach and its potential impact takes careful attention and time. We work hard to publish accurate and trustworthy reports, ensuring everybody who reads them understands their seriousness.

We quickly established that the VPNs using the exposed database and server most likely shared a common developer and owner.

The snippet of log data displayed below is a sample taken from the database. It shows the package names for numerous VPN apps writing user data to the unsecured server. The package names all share a similar template.

Some of the VPN package names also appear in the URL for the apps on Google Play, while others may be for Windows or Mac versions of the same app.

"{\"code\": 0, \"msg\": \"ok\", \"result\": {\"wifisecurity.ufovpn.android\": \"2.3.9\", \"ufovpn.unblock.proxy.vpn\": \"4.4.4\", \"wifisecurity.ufovpn.mac\": \"3.3.0\", \"wifisecurity.ufovpn.windows\": \"3.3.0\", \"wifisecurity.ufovpn.web\": \"1.0.0\", \"wifisecurity.ufovpn.lite.android\": \"3.2.8\", \"wifisecurity.ufovpn.basic.android\": \"3.3.4\", \"ufovpn.free.unblock.proxy.vpn\": \"3.3.9\", \"com.rabbitvpn.vpn\": \"1.0.4\", \"vpn.fastvpn.freevpn\": \"1.2.6\", \"hotspot.vpn.freevpn\": \"1.3.7\", \"unlimited.securevpn.freevpn\": \"1.2.5\", \"com.free.vpn.unblock.proxy.supervpn\": \"1.1.7\", \"fast.umlimited.supervpn.proxy\": \"1.2.3\"}}"

For example, in the snippet above, the package name *"com.freevpn.fast.unlimited.proxy"* appears in the URL for Free VPN's Google Play app page *("https://play.google.com/store/apps/details?id=com.freevpn.fast.unlimited.proxy").*

The same package name is also connected to the VPN's website URL *"http://free-vpn.io/".*

Similarly, the package name *"vpn.fastvpn.freevpn"* appears in the URL for Free VPN's Google Play page *("https://play.google.com/store/apps/details?id=vpn.fastvpn.freevpn").*

The website for this app is "*https://www.fastvpn.im/".*

To confirm our initial findings, **we ran a series of tests using UFO VPN.** After downloading it to a phone, we used the UFO VPN app to connect to servers around the world.

Upon doing so, new activity logs were created in the database, with our personal details, including an email address, location, IP address, device, and the servers we connected to.

Furthermore, **we could clearly see the username and password we used to register our account,** stored in the logs as cleartext.

This confirmed that **the database was real and the data was live.**

Reaching Out to the VPN Developers

Over a week, we reached out to four of the VPNs and their developers, along with Hong Kong's Computer Emergency Response Team (HKCERT) office, and, eventually, numerous tech journalists (who often have better experiences interacting with companies).

We hoped to share our findings on the nature of the leak and work quickly with all those involved to ensure the exposed data was secured.

However, **we faced considerable obstacles** in doing so.

Initially, on July 5th, we contacted the customer support at the companies marketing four of the VPNs, along with the developers of the VPNs themselves:

Dreamfii HK Ltd (UFO VPN); Mobipotato HK Limited (FAST VPN), Starxmobi HK Ltd (Free VPN), and Nownetmobi (Super VPN).

Mobipotato responded quickly but seemed unaware of the issues that come with an unsecured server – especially one that contains information they're not supposed to be recording – and didn't understand what "PIIs and its affections" are.

We sent two replies to the company twice but **received no further communication.**

On July 7th and 9th, we attempted contact with numerous people at Dreamfii, the developers of UFO VPN, to no avail.

In the meantime, **we also contacted HKCERT to notify them of the leak.** We received the following reply from HKCERT on July 13th:

"We have notified the ASN of the IP you mentioned for follow-up. Since the country of the IP location is US, and the log you provided cannot show the information is related to Hong Kong. Would you please contact US-Cert for help or provide more information indicates that the data leakage incident is related to Hong Kong?"

We made two more attempts at contacting individuals working at Dreamfii directly, including its Company Director.

The journalists we enlisted to help us experienced similar difficulties in reaching out to the companies responsible for the VPNs in question, but eventually received some replies to their inquiries.

On July 15th – 10 days after we initially reached out – **we independently verified that the database had been secured and was no longer leaking user logs.**

The same day, **we received the following response from the UFO VPN Team:**

"1. Due to personnel changes caused by COVID-19, we've not found bugs in server firewall rules immediately, which will lead to the potential risk of being hacked. And now it has been fixed.

2. Potential risk time: Jun 29 – Jul 13
3. We do not collect and restore users' home addresses. In this server, all the collected information is anonymous and only be used for analyzing the user's network performance & problems to improve service quality. Some feedbacks sent by users themselves contain email, however, the number is very small, less than 1% of our users.
4. 'clear text passwords' are not the password for logging in their accounts. It must be the tokens to connect VPN servers, and we collect it within feedback from users to check if the wrong token is applied. We name it "password" in feedback and store it in cleartext. But for user accounts and logging-in passwords, we have all of them encrypted when transferring and storing."

However, based on our investigation, **we concluded this statement was incorrect** and replied with further evidence to back this up.

Example of Data Entries

Throughout our investigation, **the exposed server was still live, with recent entries included in the logs.**

The server's data evidently belongs to the systems and users of UFO VPN, Fast VPN, Free VPN, Super VPN, Flash VPN, and RabbitVPN. In most cases, the data entries we found were not limited to just one VPN, but instead were related to all of them.

Clear Text Passwords

We found logs that contained – in clear text – **the email address of users and their passwords for account registration,** password change requests, and failed login attempts.

New user registration logs for certain VPNs

Fast VPN new user registration log

Record of a user from Bangladesh changing their password – shows an old and new password

Logged Web Activity and Technical Details

Our team found entries within **the exposed database containing a lot of personal details about users and technical information about the devices** on which the VPNs were installed, including:

- Connection logs, traffic, and sites visited
- Origin IP addresses
- Internet Service Provider (ISP)
- Actual location
- Device type
- Device ID
- App version
- Phone models

- User network connection

The VPN server users connected to was also exposed, including its region and IP address. **This makes the affected VPN service virtually useless,** as the user's origin IP address can be connected to their activity on the target server.

User from Tehran, Iran

```
▼ 4:
    _index:          "[redacted]-2020.06.20"
    _type:           "_doc"
    _id:             "[redacted]"
    _score:          1
  ▼ _source:
      ch_mode:       "AUTO"
      client_ts:     [redacted]
      ss_country:    "Germany"
      ss_type:       0
      ip_operator:   "MTNIrancellTelecommunicationsServicesCompany"
      heart_users:   -1
      host_name:     "ufo-launch-server1"
      txid:          "[redacted]"
      sim_operator:  ""
      broken_cnt:    0
      conn_random:   0
    ▼ agent:
        name:        "ufo-launch-server1"
        version:     "7.1.1"
        id:          "[redacted]"
        ephemeral_id: "[redacted]"
        hostname:    "[redacted]"
        type:        "filebeat"
      used_ts:       2402531
      conn_result:   1
      @timestamp:    "2020-06-20T07:31:36.716Z"
      phone_country: "IR"
      app:           "fast android"
      client_ip:     "[redacted]"
      device_id:     "[redacted]"
      avg_delay:     548
      ip_isp:        "Iran Cell Service and Communication Company"
      conn_way:      "direct"
      ss_city:       "Dusseldorf"
      client_os:     "android"
      ss_domain:     ""
      ip_region:     "Tehran"
```


Another user from Tehran, Iran

Connection log of user from Khartoum, Sudan

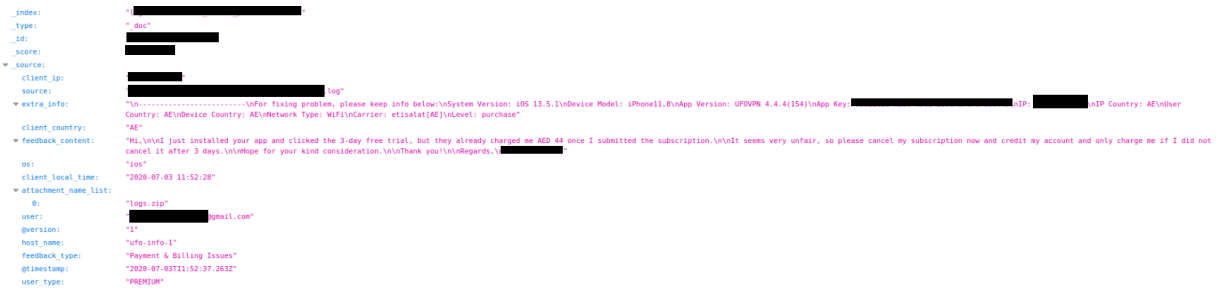
In some cases, **illicit sites were accessed from countries where viewing such content is an illegal and punishable activity.**

Iranian user accessing adult content via the VPN

Additional user web activity log

User Support Messages

Included in the leaking server were **multiple messages from users to the VPNs' customer service agents, particularly those complaining about the lack of support and fraudulent charges** from the VPN company itself.



Payment Information Logs

Sensitive Paypal API links were logged alongside the full names, emails, and addresses of users using this payment method with the assumption that it will be more secure. Those using cryptocurrency are also recorded in logs that identify them by their email and other identifiers.

Paypal payment log of a user based in the USA

Cryptocurrency payment log of a user based in France

Huawei-labeled data

Our team found instances of **Huawei-labeled data entries not only related to users' devices.** In the recent past, Huawei has been accused of spying on American customers through their devices.

Entries labeled with Huawei data

Entries labeled with Huawei data

Personally Identifiable Information (PII) Data

There was no shortage of PII data in this server leak. It included:

- Full names
- Users' home or work addresses
- Users' origin IP address as well as the IP address of the VPN server they connected to
- VPN account login credentials (email, username, password)

This log shows the full names for both the account holder and payer – two different individuals, who are representatives of a foreign embassy based in Turkmenistan.

Internal Data & Logs

The server was also being used to store internal data from some of the VPNs, including entries from their Customer Relationship Management (CRM) software, as well as all of the activity between the VPN app users and the company's platform (including registration, speed tests, password changes, etc.)

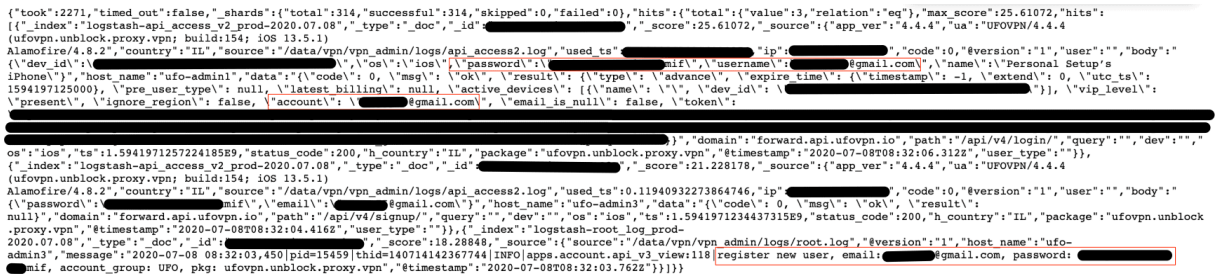
Results from Our Test

The following screenshots show various data points from our test of the UFO VPN app. They confirm **the database was live and the contents were real.**

Activity log from our test

Entry shows us connecting to a server in Milan, Italy

Entry shows us connecting to a server in London, England



Data showing our VPN account details

Data Breach Impact

The multiple VPNs sharing this single server seem to have been created and white-labeled by the same entity. Regardless of the different branding for each, they should not use their anonymity to take advantage of users duped into trusting their claims.

Impact on VPN users

Phishing and Fraud

Using the PII data exposed through the ElasticSearch server, **malicious hackers and cybercriminals could create very effective phishing campaigns** targeting the users of the exposed VPN apps.

A phishing campaign involves sending fake emails to a target, imitating a real business. These emails aim to **trick victims into providing sensitive financial data, such as credit card details, or clicking a link embedded with malicious software** like malware and ransomware.

Utilizing the leaked payment data of either the Paypal or Bitcoin payment methods, there is enough for a trained digital thief to take advantage of these VPNs users' finances through these platforms.

If any of the criminal schemes described above were successful, the **impact on a victim's personal life and financial welfare could be devastating,** especially during a global pandemic, with so much uncertainty, growing unemployment, and a looming recession.

Blackmail, Extortion, and Doxing

VPN users rely on the privacy and anonymity a VPN provides for many reasons. But the most important benefit is keeping both your online activity and identity hidden, and separate.

A VPN should never connect a person's browsing to their identity in any way. However, these VPN apps did precisely that through their activity logs, and they've exposed the details to the public.

In doing so, they compromised the safety and security of their users.

If malicious hackers had access to the VPN records, they could target users for blackmail and extortion, threatening to expose their private, potentially embarrassing activity to friends, family, colleagues, and in some cases, their government and police agencies (see below).

By threatening to 'dox' vulnerable VPN users in this way, hackers could **extort vast sums of money,** and create terrible trauma and stress for a victim, potentially ruining their life.

This form of **abuse and blackmail could continue for years,** as the blackmailers could simply store the records and threaten to release over and over again.

Arrest or Persecution

As outlined previously in the report, many of the millions of **VPN users exposed in this leak live in countries with violently repressive governments, such as Iran and Sudan.**

The threat of government surveillance and arrest for innocently using the internet is why VPNs are so popular in these countries in the first place.

By recording their users' activities and logging so much of their PII data, despite explicitly promising not to, **these VPNs have betrayed their most vulnerable users and exposed them to great danger.**

Had the records we viewed been leaked onto the dark web or shared openly, **repressive governments could use them to target users in their country for arrest, detention, and imprisonment.**

Impact on the affected VPN apps

The most immediate issue for the VPNs themselves is **the potential loss of users.** Users could abandon the VPNs in huge numbers, if they **no longer trust the developers to follow basic security protocols** or abide by their own privacy policies.

The consequences could be financially devastating for the VPNs and their parent company, not to mention the **negative publicity and press attention gained from**

the leak. It will be incredibly challenging to overcome the bad news and tarnished reputation a leak of this magnitude could cause.

Had malicious hackers discovered the exposed database, they could have targeted the VPNs themselves for fraud, viral attack, and much more.

There's no knowing what kind of impact such actions would have had, but the VPNs would undoubtedly have been undermined, and **their entire network and user base exposed to danger.**

Finally, the VPNs could face legal **issues or aggressive action from the repressive governments whose citizens are using their software.** They may be banned from certain markets or targeted with specific restrictions to block their ability to operate.

Advice from the Experts

For the VPN App Developers

The developers of these VPNs could have easily avoided this leak if they had taken some basic security measures to protect the database. These include, but are not limited to:

1. Securing its servers.
2. Implementing proper access rules.
3. Never leaving a system that doesn't require authentication open to the internet.
4. Refrain from logging sensitive, personal user data unless necessary. If logging this data is required, it should be encrypted in accordance with the highest security standards.

Any company can replicate the same steps, no matter its size.

For a more in-depth guide on how to protect your business, check out our guide to securing your website and online database from hackers.

For VPN Users

If you're using one of the VPNs affected in this data leak, we suggest switching to a more secure provider.

There are some excellent free VPNs that don't compromise on security and follow strict privacy protocols.

However, **even the best free VPN has severe limitations and can be incredibly frustrating to use,** due to slow speed, pop up ads, and worse.

If you really want to stay hidden online and have complete peace of mind that your VPN isn't putting you in jeopardy, check out your guide to the absolute best VPNs available.

How and Why We Discovered the Breach

The vpnMentor research team discovered the breach as part a huge web mapping project. Our researchers use port scanning to examine particular IP blocks and test different systems for weaknesses or vulnerabilities. They examine each weakness for any data being exposed.

Our team was able to access this database because it was completely unsecured and unencrypted.

Whenever we find a data breach, we use expert techniques to verify the owner of the database.

As ethical hackers, we're obliged to inform a company when we discover flaws in their online security. We reached out to the developers, not only to let them know about the vulnerability but also to suggest ways in which they could make their system secure.

These ethics also mean we carry a responsibility to the public. Users of the VPN apps must be aware of a data breach that exposes so much of their sensitive data. The purpose of this web mapping project is to help **make the internet safer for all users.**

Introducing The Leak Box

To ensure our mission has the most significant impact possible, **we've also built The Leak Box.**

Hosted on the dark web, the Leak Box **allows ethical hackers to anonymously report any data breach they find online.** We then verify and report any submission deemed a legitimate threat to the public's safety.

We never sell, store, or expose any information we encounter during our security research. This includes any information reported to us via The Leak Box.

About Us and Previous Reports

vpnMentor is the world's largest VPN review website. Our research lab is a pro bono service that strives to help the online community defend itself against cyber threats while educating organizations on protecting their users' data.

Our ethical security research team has discovered and disclosed some of the most impactful data leaks in recent years.
This has included an enormous data leak exposing credit cards, government IDs, and more belonging to millions of US citizens. We also revealed that a popular online learning platform compromised the privacy and security of people across the globe. You may also want to read our VPN Leak Report and Data Privacy Stats Report.