golden frog

VyprVPN No Log Assessment

Final Report

limitless innovation. no compromise.

Prepared for: Michael Douglass
Chief Scientist

Golden Frog
2500 Bee Cave Road
Building 1, Suite 400
Austin, TX 78746-6943
United States

11/9/2018

Version:	Final Report with Retest Results
Prepared for:	Golden Frog
Date:	11/9/2018
Prepared by:	Joel Voss, Ryan O'Neill, Dr. Crispin Cowan, and Mark Stribling

Table of Contents

Executive Summary

Golden Frog engaged Leviathan Security Group in September 2018 to evaluate updates to its VyprVPN product with the goal of providing "No Log" VPN service to customers. Specifically, Leviathan reviewed the platform to ensure that no Personally-Identifiable Information (PII) about customers with respect to their use of the service are logged by Golden Frog except as required for business operations.

Golden Frog seeks to reduce the exposure of their clients by providing VPN service with an explicit guarantee that it does not log connection details. It designed the various clients to report information about connections by default, but that connection data is anonymized and can be turned off by user configuration. Connections are logged during authentication, but logs that could identify users are kept only for a short time. By using open source or widely-used applications for server and client components, they have reduced the risk of unintentionally adding a weakness into the software themselves.

Observations

The VPN clients produce no identifying logs without the user's consent. There were a limited number of identifying logs on the VPN server which appeared result from inadvertent configuration mistakes. Specifically, we found that logs for the kill switch API contained user IP addresses.

We considered a wide range of attackers that might be interested in deanonymizing VPN users. The most common ones would be an ISP attempting to learn about the browsing habits of a user, or content producers seeking to restrict activity to a geographic region. The most powerful attackers would be nation states that may wish to determine the source of a leak. While VPNs should not be considered an effective defense against highly-sophisticated attackers, they can reduce those attackers' options from surreptitious gathering of intelligence to issuing a writ to force a company to spy on their users.

We examined all components of the project according to the threat assessment described below. While vigilance against logging is necessary to complete the process of implementing "No Log", we feel that this assessment achieved its goal of uncovering weaknesses in Golden Frog's implementation. The project revealed a limited number of issues that Golden Frog quickly fixed. As a result, it can provide VyprVPN users with the assurance that the company is not logging their VPN activity.

Recommendations

Golden Frog worked to remediate all no-log-related findings concurrently with the assessment. Once it had completed this, we performed a retest and *verified that all of the fixes were effective*.

In the long term, we recommend that Golden Frog continue to monitor their servers for regressions. This can be done manually as part of maintenance or automatically by creating an alert that triggers on test data being recorded in logs. Since Golden Frog already has test accounts, they could use these to grep logs for IP, username, and user ID. While this will not find different encodings or data that could be combined to deanonymize a user, it avoids the most common case where a configuration change results in a regression to the default behavior.

Findings Index

This section represents a quick view into the findings discovered in this assessment.

SEVERITY	TITLE	COMPONENT	ID	STATUS
High	Sensitive information in openvpn.log	VPN	83898	**Fixed**
High	Sensitive information in ppp-connect.log	VPN	83900	**Fixed**
High	Splunk servers contain sensitive log data (usernames and IPs)	Cruncher/Logs and Splunk	83869	**Fixed**
Medium	Sensitive information in dmesg	VPN	83899	**Fixed**
Medium	Sensitive information in killswitch.log	VPN	83901	**Fixed**
Medium	URL path in DAPI logs	DAPI	83868	**Fixed**

Log Finding Classification

Impact	When we find logging of PII, we assign it one of five categories of severity, essentially describing the potential impact if it was abused: Informational only – We found a condition that doesn't present a current threat, but it could create one in the future if certain changes are made. You'll probably want to fix it. Low – The log might allow an attacker to gain information that could be sensitive. However, it doesn't allow direct access to data or resources. Medium – The log may result in an activity being connected to a user. High – The log reveals all information or activity of a user. Critical – The log reveals all information about all users.
Skill Level to Exploit	When we find logging of PII, we also assess what authority a user must have to gain access to it: Simple – Only a minimal understanding of the underlying technology is required. Tools and techniques for accessing it can be easily found on the Internet. Moderate – The data is not available to all users, but it is available to employees. It is available to attackers who are able to exploit a vulnerability. Advanced – Near-complete and superior understanding of the technology involved is required. Direct interaction with the victim or target may also be required.

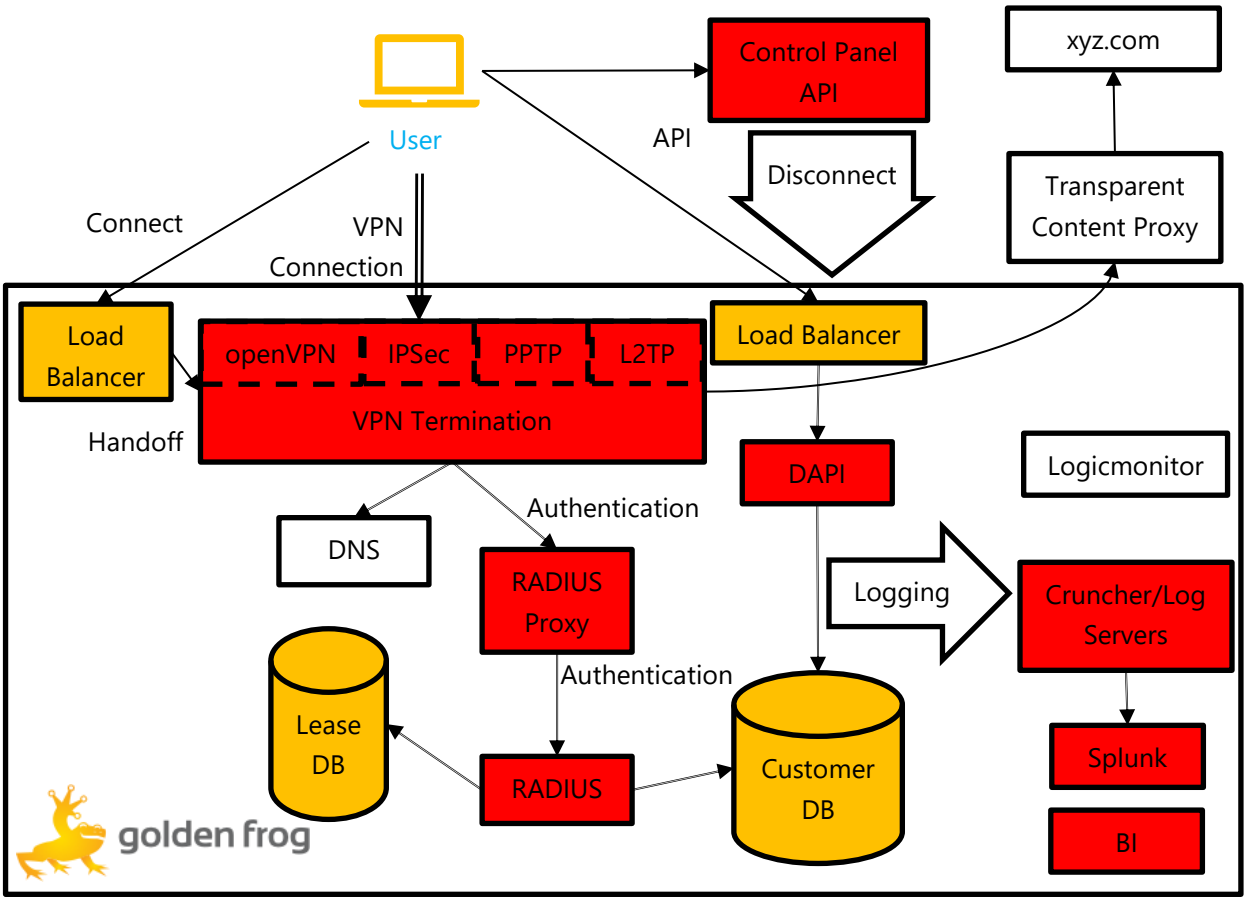
Impact Rating (Weight)	Authority Level to Access Rating (Weight)		
	Advanced (1)	Moderate (2)	Simple (3)
Critical (4)	4	8	12
High (3)	3	6	9
Medium (2)	2	4	6
Low (1)	1	2	3

Severity	
Critical	10-12
High	7-9
Medium	4-6
Low	1-3

Threat Assessment and Scoping

This engagement was notably *not* a security evaluation, but rather focused on privacy. The goal was to determine whether VyprVPN was logging user activities. Golden Frog explicitly seeks to avoid logging any sensitive activity related to its users use of the VyprVPN service. As such, the singular "threat" under consideration is the propensity of the specific software components used by VyprVPN to perform logging which can associate a user with a specific VyprVPN session or to any activity during the session, and whether Golden Frog was successful in removing or mitigating that logging.

The system looks like this. We collapsed complex components into a single box in the figure when we determined that they comprise a single *security principal*[1]. The components have been colorized with respect to the level of threat presented to that component. Red indicates a major threat in that the component has full data on the user's current activity and could log it. Orange indicates a minor threat in that the component has *some* user data that could be concerning and could be logged. Normal black text indicates that the component is not at significant risk of logging user activity, because the component does not have the data. Blue indicates components that *would* be a security risk but are out of scope for a specified reason.



[1] A set of components that all have exactly the same set of access and privileges https://en.wikipedia.org/wiki/Principal_(computer_security)

- **User:** This is the customer/user of the VyprVPN service. The user's activities are outside of Golden Frog's control, but the client software is provided to the user by Golden Frog. Golden Frog offers client applications for Windows, MacOS, iOS, and Android. The client software is a **moderate risk** of logging, in that it does actually log a great deal of information, but it does not *export* that information unless the user consents. In several cases, it is not possible for Golden Frog to prevent the logging, because the OS platform does not provide options to disable logging. The software should be inspected to assure that logs are *only* exported with user consent.
- **Load Balancers:** Users connect to the Load Balancer which uses standard networking techniques to hand the connection off to the VPN Termination server. The user's connection to the Load Balancer is thus only momentary, but none the less the Load Balancer witnesses a user connecting to VyprVPN, and so is a **moderate risk** of logging.
- **VPN Termination:** The client communicates with the VPN Termination server via one of 4 protocols (OpenVPN[2], IPSec[3], PPTP[4], and L2TP[5]). The user first authenticates to the VPN termination point, which then negotiates a VPN connection with the user's client software. The VPN Termination node is a **high risk** of logging, because upon connection and throughout the session, it is in full possession of the user's identity and activities. The software was inspected to assure that it does not log these activities. Special consideration was made to differentiate between Connection State information which lives for the duration of a connection vs. Logged information kept after the termination of a session.
- **DAPI:** In the course of operations, the client software calls various APIs offered by Golden Frog and is served by the DAPI node. DAPI is a **high risk** of logging, because upon calling its APIs, it is in full possession of the user's identity and activities. The software was inspected to assure that it does not log these activities in association with the identity of a user.
- **RADIUS Proxy, RADIUS:** The VyprVPN Termination servers authenticate VyprVPN customers using the RADIUS protocol. The VPN Termination node use the RADIUS Proxy/Server running on the VyprVPN Termination server itself to load-balance the RADIUS request to the RADIUS servers in the site. The RADIUS proxy and server are a **high risk** of logging, because upon connecting to VyprVPN, it is in full possession of the user's identity, the Client IP, the Lease IP, and the time at which the user connected. The software was inspected to assure that it does not log authentication events in a way which allows the association of a user with a session. **Note** that *not* logging authentication attempts and successes is itself a security threat, and so Golden Frog has a very challenging conflict of competing interests here.
- **Lease DB:** RADIUS uses the Lease DB to manage user network leases. The Lease DB is a **moderate risk** of logging, because it stores the user's assigned IP address for network management purposes for the duration of the connection. The Lease DB was inspected to assure that the data it stores is the minimum required to achieve functional objectives, and that the data is not persisted any longer than necessary.

---

[2] https://openvpn.net/index.php/open-source.html
[3] https://en.wikipedia.org/wiki/IPsec
[4] https://en.wikipedia.org/wiki/Point-to-Point_Tunneling_Protocol
[5] https://en.wikipedia.org/wiki/Layer_2_Tunneling_Protocol

- **Customer DB:** RADIUS and DAPI both use the Customer DB to manage customer status, such as credentials and billing status. The Customer DB is a **not at risk** of logging, in that it is a read-only database of customers. Customer information is a privacy concern, but Golden Frog is only promising not to log customer *activity*; the fact that a person is a Golden Frog customer is necessarily logged for authentication and payment purposes.
- **Control Panel API:** Golden Frog uses two private API endpoints to allow customers to disconnect their connections via a central web control panel. The endpoints access the lease database and, if necessary, make a request to the VPN process itself to terminate a connection. Requests originate from the Golden Frog website server in Zurich. These requests and the responses may include the customer's identity and their lease IP address. As a result, these endpoints are **high risk** of logging. The software was inspected to verify that neither the responses nor the requests log any of this information. The serv/vyprapi systems takes the request and then contacts the Control Panel API on the proper vpn/vyprnode system to do the actual work.
- **DNS:** VyprVPN offers a private DNS resolver, so that user's DNS queries are decoupled from the user. The VyprVPN DNS server in turn queries the Internet to resolve DNS queries, sourcing the DNS request from the appropriate geographic node. The DNS resolver works in two stages: A local DNS forwarder runs in each site. Customer DNS requests go to this forwarder first and come from the Lease IP of the VPN connection. The forwarder then sends the DNS request to an in-country VM; the in-country VM has zero knowledge of the user because all requests come from the DNS forwarder IP address. The DNS resolver is **not at risk** of logging, because it never has possession of specific user identities causing the requests that it serves.
- **Transparent Content Proxy:** The Transparent Content Proxy is **not at risk** of logging, because it never has specific customer identities.
- **LogicMonitor:** This is a system monitoring log server, used by Golden Frog to manage performance and resource allocation. It does not handle specific-user data, instead logging activities like CPU and disk utilization, availability, and server timings. Thus, LogicMonitor is **not at risk** of logging because it does not have any user-specific data.
- **Cruncher/Logs, Splunk:** These nodes are used for detailed system logging, and thus well could be storing specific user activity events. Sanitizing logs of user-specific activity is notoriously difficult[6], and so they are a **high risk** of logging.

Project Components and Descriptions

From the threat assessment above, these are the project components to be evaluated and how we assessed each one.

CRUNCHER/LOGS, SPLUNK	Inspect to assure that it is not logging particular user activities, and that user activities cannot be inferred from the logs it does record

[6] https://en.wikipedia.org/wiki/Netflix_Prize#Privacy_concerns

VPN TERMINATION & CONTROL PANEL API	Inspect to assure that it is not logging user connections
DAPI	Inspect to assure that it is not logging user API calls
CONTROL PANEL API	Inspect to assure that it is not logging user API calls
RADIUS PROXY AND SERVER	Inspect to assure that it is not logging user authentication
USER CLIENT APPLICATION	Inspect to assure that the logs it stores are not exported without user consent
LEASE DB	Inspect to assure that it is only storing the minimum user information necessary for functional objectives, and not persist longer than necessary
LOAD BALANCERS	Inspect to assure that the load balancers do not log connections as they handle user requests and pass them along to actual servers

Observations & Analysis

The following sections describe the results of our evaluation of each component.

Cruncher/Logs and Splunk

VyprVPN uses Cruncher/Logs to send event logs to Splunk[7]. Splunk is a product that collects data and log-files from remote machines and presents the data via a Web interface that allows for queries and searches. Splunk can also be used to filter data found in logs, and create complex pattern matching statements for omitting, mutating, removing or augmenting the data that it is collecting. The Splunk forwarders were running on two servers `cruncher1` and `logs1`.

Threat Analysis

Some log events are important to Golden Frog and harmless to users, such as when a particular disk drive is full or has failed. Others would constitute a violation of the "no log" promise to customers, such as failed login attempts by legitimate users mistyping their password.

Methodology

Golden Frog did not provide source code for Cruncher nor Splunk as they are 3rd party products. Instead we were able to observe configuration files on the Splunk servers. We also analyzed their respective Linux environment to look for sensitive logging data. We searched for unsafe permissions on log data and core file `ulimit` settings. We also used simple pattern matching searches against the log files in various locations.

Observed Trends

The Splunk servers both have coredumps explicitly disabled; `ulimit -c` is set to `0`. Coredumps from Splunk would have all the recent logs stored in the process memory of the data segment, heap and stack and would thus be logged within the core file itself.

The Splunk configuration itself is fairly complex and we did not ascertain every nuance of its configuration. However, we did observe that log-files appeared to be sanitized by the time they reach the Splunk server. That said, there were several locations on the 'logs1' server where log-files contained sensitive user data including usernames and IPs (83869). The retest confirmed that Golden Frog addressed this issue.

[7] https://www.splunk.com/

Findings

SPLUNK SERVERS CONTAIN SENSITIVE LOG DATA (USERNAMES AND IPS)

ID	83869
Component	Cruncher/Logs and Splunk
Severity	**High**
Impact / Skill Level	High/Simple
Reference	N/A
Location	logs1.ams1:/opt/logs/vyprvpn/ppp-connect.log
Status	**Fixed**

Observation

The application does not take measures to sanitize sensitive information out of the log output. In the following log-files we found usernames in the form of username@email.com, along with two Golden Frog IP addresses; the called_ip and the nas_ip.

```
ppp-connect.log
vpn-disconnect.log
vpn-connect.log

Oct  9 06:11:28 vyprnode116.ams1.goldenfrog.com ip-down.local: client-
disconnect success, username=<email address> protocol=pptp pppdevice=ppp6
nas_ip=10.102.113.116 framed_ip=31.6.27.110

Oct  9 03:35:07 vyprnode13.ams1.goldenfrog.com ip-up.local: client-connect
success, username=<email address> protocol=l2tp pppdevice=ppp5
nas_ip=10.102.113.13 framed_ip=128.90.24.87

Oct  9 03:35:03 vyprnode96.ams1.goldenfrog.com ip-down.local: client-
disconnect start, username=<email address>|waa protocol=pptp pppdevice=ppp2
nas_ip=10.102.113.96 framed_ip=31.6.32.86
```

Recommendation

Make sure that all logs are properly sanitized so that there is no usernames or other sensitive information being logged.

VPN Termination

This node is the termination point for VPN services. It serves connections via OpenVPN, IPsec, PPTP, and L2TP. It also is the front face of user authentication, validating that a requesting user is actually a VyprVPN customer.

Threat Analysis

The VPN termination node has complete awareness of all user activities:

- Initial connection
- Authentication
- All network traffic
- DNS requests
- Termination

It is vital that VPN not log this user activity.

Methodology

We viewed the components of the system and reviewed any modifications necessary for commercial use. We then logged into two production servers provided for testing and checked their configuration. Then we checked running processes to determine what files might be in use. We looked at each log file manually and grepped for usernames (which have a common format), user IDs, and IP addresses (which are regular) being logged. We checked the operating system for any logging mechanism that could be used to track user activities.

Observed Trends

The design of the system uses off-the-shelf servers (StrongSwan, OpenVPN, OpenL2TPd, and pptpd) with modifications to fit into this commercial use case. Because these servers are off-the-shelf, they are prone to logging information that users would prefer to be private. These behaviors need to be modified to get the desired result. In the case of OpenVPN, PPTP, and L2TP, we found that logging of usernames occurred (83898 and 83900). This can be explained by the fact that configuration management might not be sufficiently rigorous. We also found that dmesg was logging IP addresses (83899).

The retest confirmed that Golden Frog successfully addressed all issues in VPN termination.

Findings

SENSITIVE INFORMATION IN OPENVPN.LOG

ID	83898
Component	VPN
Severity	**High**
Impact / Skill Level	High/Simple
Reference	N/A
Location	vpn1.tor.goldenfrog.com vyprnode1.ams1.goldenfrog.com /var/log/vpn/openvpn.log
Status	**Fixed**

Observation

The application does not take measures to sanitize sensitive information out of the log output.
The log contains email address and IP address of the user.

```
Oct  8 03:27:48 vpn1.tor.goldenfrog.com openvpn: Mon Oct  8 03:27:48 2018
<email address>|waa/<ip address>:63655 WARNING: 'link-mtu' is used
inconsistently, local='link-mtu 1570', remote='link-mtu 1602'

Oct  9 03:20:06 vyprnode1.ams1.goldenfrog.com openvpn: Tue Oct  9 03:20:06
2018 <email address>|maa/<ip address>:1194 WARNING: 'link-mtu' is used
inconsistently, local='link-mtu 1570', remote='link-mtu 1602'
```

Recommendation

Check all instance of calling a log writer to make sure that sensitive information such as username and IP are not being logged.

SENSITIVE INFORMATION IN PPP-CONNECT.LOG

ID	83900
Component	VPN
Severity	High
Impact / Skill Level	High/Simple
Reference	N/A
Location	vyprnode1.ams1.goldenfrog.com /var/log/vpn/ppp-connect.log
Status	**Fixed**

Observation

The application does not take measures to sanitize sensitive information out of the log output
The ppp-connect.log logs usernames and IP addresses.

```
Oct  8 06:42:36 vyprnode1.ams1.goldenfrog.com ip-up.local: client-connect
start, username=<email address> protocol=pptp pppdevice=ppp3
nas_ip=10.102.113.1 framed_ip=<IP address>
```

Recommendation

Check all instance of calling a log writer to make sure that sensitive information such as usernames and IP addresses are not being logged.

SENSITIVE INFORMATION IN DMESG

ID	83899
Component	VPN
Severity	Medium
Impact / Skill Level	High/Moderate
Reference	N/A
Location	vpn1.tor.goldenfrog.com dmesg
Status	**Fixed**

Observation

The application does not take measures to sanitize sensitive information out of the log output.
The kernel logs IP address and port of systems that send packets with a bad checksum. This can be used to identify users because UDP packets will have a random mutation over time. Users of the VPN will eventually send a packet with a bad checksum.

```
dmesg
[77274.828361] UDP: bad checksum. From <IP address>:51601 to <IP
address>:16802 ulen 108
```

Recommendation

Check all instance of calling a log writer to make sure that sensitive information such as IP address and username are not being logged.

DAPI

DAPI is an API server, used by the VyprVPN client software to manage the user's service.

Threat Analysis

The DAPI node has awareness of a subset of the user activities exposed to the VPN node

- Initial connection
- Authentication
- Termination

It is important that VPN not log this user activity.

Methodology

We started the test by reading the source code to find what the system did and where logging could occur. We requested data from the server and recorded the responses. We were provided a trial premium account, so we used the credentials to make authenticated requests to the server. We logged into the web server and checked for configuration and logs in the place where Apache is configured to store logs. We additionally looked in the syslog and other system logs for evidence of users. We looked at processes running to ensure that the system did not have any software that would create logs besides Apache.

Observed Trends

The DAPI is a web service built on Flask with authentication of certain necessary endpoints. It is used for unauthenticated calls to /vyprvpn/locations which provides users with a list of servers they can connect to. It is also used for authenticated calls to /vyprvpn/settings.

We found that IP addresses were logged in the DAPI when a user intentionally wrote them into the request (83868). This is not part of the client software, so it would need to be a leak of information by a programmer who decided to use it to their own ends.

The retest confirmed that Golden Frog successfully addressed this issue in DAPI.

Findings

URL PATH IN DAPI LOGS

ID	83868
Component	DAPI
Severity	**Medium**
Impact / Skill Level	Medium/Moderate
Reference	N/A
Location	https://api.goldenfrog.com/vyprvpn/connections/50.78.42.169ffff
Status	**Fixed**

Observation

The application does not take measures to sanitize sensitive information out of the log output
The request URL is logged as seen in the following request and log:

```
sudo tail -f /var/log/nginx/access.log |grep '50\.78'
- - - [05/Oct/2018:17:59:23 -0500] "/vyprvpn/connections/50.78.42.169ffff"
500 291 "-" "-" "-"

curl -i -H 'X-Real-IP: 127.0.0.1' -d '{"disconnect":"0", "userid":"0"}'
https://api.goldenfrog.com/vyprvpn/connections/50.78.42.169ffff; echo
HTTP/1.1 500 INTERNAL SERVER ERROR
Server: nginx/1.10.2
Date: Fri, 05 Oct 2018 22:59:23 GMT
Content-Type: text/html
Content-Length: 291
Connection: close

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<title>500 Internal Server Error</title>
<h1>Internal Server Error</h1>
<p>The server encountered an internal error and was unable to complete your
request.  Either the server is overloaded or there is an error in the
application.</p>
```

While normal requests to /vyprvpn/connections/<ip> do not result in a log being created (for an unknown reason), requests that cause an error such as the above are logged in the access log.

Recommendation

Check all instance of calling a log writer to make sure that sensitive information such as IP addresses and usernames are not being logged.

Control Panel API

Control Panel API is a special server that allows VyprVPN clients to call it to terminate connections, where ever they may be.

Threat Analysis

The Control Panel API node has awareness of a subset of the user activities exposed to the VPN node, notably:

- Kill switch activation

It is important that VPN not log this user activity as it contains a timestamp and IP address.

Methodology

We logged into the VPN server and reviewed source code for the kill switch and control panel. We checked for configuration and logs in the place where nginx is configured to store logs. We additionally looked in the syslog and other system logs for evidence of users. We looked at processes running to ensure that the system did not have any software that would create logs besides nginx, Unicorn, and Python. We checked that the API could not be called directly by users. We made requests to the server from localhost and checked the resulting log for data leakage.

Observed Trends

The Control Panel API is a minimal, unauthenticated interface accessible only to servers and developers. It has a handful of simple functions which connect directly into the heart of the VPN. We noticed that the kill switch logged IP addresses (83901). The minimal design of this API does not make it invulnerable, access to it should be handled carefully to ensure that it does not grow to be abused.

The retest confirmed that Golden Frog successfully addressed this issue in the Control Panel API.

Findings

SENSITIVE INFORMATION IN KILLSWITCH.LOG

ID	83901
Component	VPN
Severity	Medium
Impact / Skill Level	High/Moderate
Reference	N/A
Location	vyprnode1.ams1.goldenfrog.com /var/log/vpn/killswitch.log
Status	**Fixed**

Observation

The application does not take measures to sanitize sensitive information out of the log output.
The log file /var/log/vpn/killswitch.log contains the IP address of the connection killed.

```
Oct  6 14:41:04 vyprnode1.ams1.goldenfrog.com killswitch:
[vpn._listener_dispatch]: KILL ['KILL', 'OpenVPN:<IP address>:62293',
'AdSr72FAdr\n']
Oct  6 14:41:04 vyprnode1.ams1.goldenfrog.com killswitch:
[vpn._listener_dispatch]: kill_result SUCCESS: connection <IP address>:62293
terminated
```

Recommendation

Check all instance of calling a log writer to make sure that sensitive information such as usernames and IP addresses are not being logged.

RADIUS Proxy and Server

VyprVPN uses a RADIUS[8] server and proxies to authenticate users. The users request access to the VPN node, which in turn connects to the RADIUS proxy, and thence to the RADIUS server, to authenticate the user as a legitimate customer.

Threat Analysis

The RADIUS server and its proxies have visibility to every login attempt, successful or not. It is normal for authentication servers to log authentication connections, for security purposes. However, logging authentication attempts would also violate the no-log promise, as it would log every time a specific customer started their VPN.

Methodology

We approached RADIUS from a holistic stand-point, starting with the configuration files for RADIUS and Docker. We looked to see what modules RADIUS was using and checked whether the configurations were using secure options. Additionally, we looked at the Python code to confirm that no unnecessary logging was performed upon connect, disconnect, or error.

We reviewed the configuration file for RADIUS proxy and looked for evidence of it logging. It did not appear to have any significant presence in the system.

Observed Trends

The code did not appear to log anything that it should not, although the configuration file in the RADIUS-module 'linelog' had a format string that appeared as though it printed PII. Upon further inspection we confirmed this was mitigated at another layer where data was filtered before being written to the logs.

The RADIUS configuration file had a security stanza where coredumps were set to disabled, which is good practice because all of the sensitive authentication data that is stored in the process memory would otherwise be dumped onto-disk in the core-file.

The RADIUS proxy does not appear to have any separate logging from the RADIUS server.

[8] https://en.wikipedia.org/wiki/RADIUS

Findings

We found no issues with the RADIUS server or RADIUS proxy.

User Client Applications

VyprVPN service requires the use of client applications to set up and operate the VPN. We reviewed client applications for the following operating systems in this review: Microsoft Windows, macOS, iOS, and Android.

Threat Analysis

In many cases, the *OS platform* does not provide options to forbid logging of activity, and so it is impossible for VyprVPN to prevent such logging on the client. Instead, VyprVPN mitigates this by only exporting such logs with explicit consent from the user, such as during a tech support case. The main threat here is whether there are residual scenarios in which the VyprVPN client app exports log data without explicit user consent. Additional threats include analytics that provide sensitive information and API calls that expose information about the user's activities.

Methodology

We installed each application in an environment suitable for test; for Android we used an Android 7 emulator, for iOS we used an iPhone running iOS 11.3.1, for macOS we used an iMac, and for Windows we used the consultant's laptop. For Android, we used `adb install VyprVpn-2.29.0.9951-RELEASE_WEBSITE.apk`. For iOS we used XCode to install VyprVPN-2.25.2.6714-Distribution.ipa. For Windows we double-clicked VyprVPN-2.14.1.8412-installer.exe. For macOS, we opened VyprVPN_v2.19.0.6517.dmg and dragged VyprVPN to Applications.

With the applications installed, we created a mechanism for intercepting HTTPS requests made by the client using the Burp web proxy. The Android and macOS clients rejected connections while iOS and Windows accepted the proxy. While this only applies when the VPN was turned off, this data was helpful in determining what data was sent from the client to any server. For Android and macOS, we used data collected from rejected connections and evaluated source code to determine what data was sent during each part of the applications' startup and disconnect. We also were able to deny a VPN connection using a firewall to gain more information about what happens when the client lacks a network with ports open for VPN (a restricted guest WiFi network).

We connected to the service repeatedly using different servers that we had access to and did not have access to. We tested IPsec, OpenVPN, and Chameleon protocols for the widest coverage of code paths. We enabled and disabled each configuration switch to see if they functioned appropriately. We made a support request while the Windows client was sending its traffic to Burp, so that we could see what data was being sent. We read any files available to us and used logcat to receive logs written by the Android client. During testing we referenced source code to ensure that we understood behavior in a broader context. Because the source codebase was large, we prioritized our coverage of the internal workings of each client.

Observed Trends

The default settings have changed in each version of the application as follows:

Help Improve VyprVPN: **on**
App Crashes: **off**
Connection Performance: **on**

With the default settings the application sent a significant amount of data to the api.goldenfrog.com server through the Mixpanel interface and the DAPI. The Mixpanel interface stripped the IP, city, and state before sending it to Mixpanel, which effectively anonymized users.

Other requests to API server occurred but were limited to login and connection which are necessary[9]. Since these requests did not log the identifying information submitted, they provided little benefit to an attacker trying to identify users. A second server app.adjust.com was used but only for infrequent requests such as creating an account or installing the application. Neither of these requests would identify a user's activity.

Logs on the clients were verbose and contained information about what the application was doing (connecting, disconnecting, and throwing errors). Since this data was private on the device, it did not represent a significant source of information for an attacker unless they gained direct access to the device.

If the user chose to send these logs to support during a support request, they could potentially leak information about their habits but not their detailed usage (what they visited, what applications they used, etc.). With all configuration checkboxes unchecked, the applications produced very few requests to Golden Frog, which is valuable to a person that has a desire for privacy (i.e., the average VPN user). For users that want to use the service without installing Golden Frog software, there is an option on each platform to install an open source application or a widely-used closed source application instead. This might provide reassurance that Golden Frog is not using the client to log information about the users. The client then can be seen as a user-friendly application to use these processes and the many servers available through VyprVPN.

Findings

We found no issues with the User Client Applications.

[9] It may not be necessary for authenticated calls to the DAPI be made to connect to the VPN, but Golden Frog has chosen to make this a part of their client software. By using https://api.goldenfrog.com/vyprvpn/locations-unauthenticated and connecting with OpenVPN or IPsec, a user can avoid using the VyprVPN client software. This method is described in Golden Frog's online documentation.

Lease DB

Lease DB stores and manages the particulars of a VPN connection *lease*, including the IP address that is assigned to the user. The database contains short-lived information about a VPN connection.

Threat Analysis

The Lease DB involves a network server, database files, and logs. If the Lease DB contained more information than it needed for the platform to function it would present a risk to user privacy. If the Lease DB logged information for a long duration, it would similarly weaken the security guarantees presented to users.

A vulnerability in the Lease DB would allow an adversary to learn about currently-connected users, which would result in the ability to create long term logs about users' status and connection properties. This would result in a correlation between activities captured on the internet being traceable back to the user.

Methodology

We reviewed the source code that interacts with the Lease DB to understand its function. We logged into the server and searched for any logs it produced. We also read the Tokyo Cabinet files it produced.

Observed Trends

The logs and database contained usernames and user IDs. This is necessary for business and is an acceptable use case. The logs and the database were correctly limited in duration and never pushed to an aggregator. Golden Frog could hash usernames and IDs, but any hash could be quickly cracked given a list of users such as exists in the customer database.

Findings

We found no issues within the Lease DB.

Appendix A – Technical Services

Leviathan's Technical Services group brings deep technical knowledge to your security needs. Our portfolio of services includes software and hardware evaluation, penetration testing, red team testing, incident response, and reverse engineering. Our goal is to provide your organization with the security expertise necessary to realize your goals.

SOFTWARE EVALUATION We provide assessments of application, system, and mobile code, drawing on our employees' decades of experience in developing and securing a wide variety of applications. Our work includes design and architecture reviews, data flow and threat modeling, and code analysis with targeted fuzzing to find exploitable issues.

HARDWARE EVALUATION We evaluate new hardware devices ranging from novel microprocessor designs, to embedded systems, to mobile devices, to consumer-facing end products, to core networking equipment that powers Internet backbones.

PENETRATION & RED TEAM TESTING We perform high-end penetration tests that mimic the work of sophisticated attackers. We follow a formal penetration testing methodology that emphasizes repeatable, actionable results that give your team a sense of the overall security posture of your organization.

SOURCE CODE-ASSISTED SECURITY EVALUATIONS We conduct security evaluations and penetration tests based on our code-assisted methodology, allowing us to find deeper vulnerabilities, logic flaws, and fuzzing targets than a black-box test would reveal. This gives your team a stronger assurance that the significant security-impacting flaws have been found and corrected.

INCIDENT RESPONSE & FORENSICS We respond to security incidents for our customers, including forensics, malware analysis, root cause analysis, and recommendations for how to prevent similar incidents in the future.

REVERSE ENGINEERING We assist clients with reverse engineering efforts not associated with malware or incident response. We also provide expertise in investigations and litigation by acting as experts in cases of suspected intellectual property theft.

Appendix B – Risk and Advisory Services

Leviathan's Retained Services group is a supplement to an organization's security and risk management capability. We offer a pragmatic information security approach that respects our clients' appetites for security process and program work. We provide access to industry leading experts with a broad set of security and risk management skills, which gives our clients the ability to have deep technical knowledge, security leadership, and incident response capabilities when they are needed.

INFORMATION SECURITY STRATEGY DEVELOPMENT We partner with boards, directors, and senior executives to shape your enterprise's overall approach to meeting information security requirements consistently across an entire organization.

ENTERPRISE RISK ASSESSMENT We develop an information asset-centric view of an organization's risk that provides insight to your organization's Enterprise Risk Management capability. This service can be leveraged with annual updates, to account for your organization's changing operations, needs, and priorities.

PRIVACY & SECURITY PROGRAM EVALUATION We evaluate your organization's existing security program to give you information on compliance with external standards, such as ISO 27000 series, NIST CSF, HIPAA, or PCI-DSS among others. This is often most useful before a compliance event or audit and helps to drive the next phase of growth for your Security and Risk Management programs.

VENDOR RISK ASSESSMENT We assess the risk that prospective vendors bring to your organization. Our assessment framework is compatible with legislative, regulatory, and industry requirements, and helps you to make informed decisions about which vendors to hire, and when to reassess them to ensure your ongoing supply chain security.

NATIONAL & INTERNATIONAL SECURITY POLICY In 2014, we launched a public policy research and analysis service that examines the business implications of privacy and security laws and regulations worldwide. We provide an independent view of macro-scale issues related to the impact of globalization on information assets.

M&A/INVESTMENT SECURITY DUE DILIGENCE We evaluate the cybersecurity risk associated with a prospective investment or acquisition and find critical security issues before they derail a deal.

LAW FIRM SECURITY SERVICES We work with law firms as advisors, to address security incidents and proactively work to protect client confidences, defend privileged information, and ensure that conflicts do not compromise client positions. We also work in partnership with law firms to respond to their clients' security needs, including in the role of office and testifying expert witnesses.

SAAS AND CLOUD INITIATIVE EVALUATION We give objective reviews of the realistic threats your organization faces both by moving to cloud solutions and by using non-cloud infrastructure. Our employees have written or contributed to many of the major industry standards around cloud security, which allows their expertise to inform your decision-making processes.

Appendix C – Leviathan Project Team

CONTACT	ROLE	EMAIL
Frank Heidt	Executive Sponsor	Frank.Heidt@leviathansecurity.com
Mark Stribling	Senior Security Project Manager	Mark.Stribling@leviathansecurity.com
Joel Voss	Senior Security Consultant	Joel.Voss@leviathansecurity.com
Ryan O'Neill	Security Consultant	Ryan.ONeill@leviathansecurity.com
Dr. Crispin Cowan	Security Consultant	Crispin.Cowan@leviathansecurity.com