Confirmed VPN Privacy Audit

Factor13 LLC | December 4-6, 2018

Confirmed offers privacy and security for law-abiding consumers while surfing the web, using apps, and other light internet use via a VPN. User privacy is crucial to Confirmed's business, and Factor13 LLC has been engaged to perform a third-party audit, resulting in this report.

Environment

Confirmed VPN operates in Amazon Web Services, predominantly using CloudFormation to manage EC2 instances. The instances themselves are instantiated from generic, public Ubuntu Server images with no Key Pair, so direct SSH access is not possible without tampering. Code is pushed to AWS CodeCommit and deployed to instances via AWS CodeDeploy. All of this is visible to third-party auditors, such as Factor13 LLC, via special-purpose AWS IAM accounts.

Architecture

VPN servers that users connect to run strongSwan to manage IPSec tunnels, Suricata to detect malicious traffic, and a small JavaScript program written by Confirmed that strongSwan invokes to check the status of a client and implement bandwidth throttling. This Bandwidth script makes HTTP calls to a Helper instance to check the status of a client ID. The strongSwan charon daemon also sends RADIUS messages to a Helper instance for bandwidth accounting. These messages include the client ID and ephemeral client IP address, but no content from them is logged by the Helper besides adding to the client's total monthly bandwidth usage tally in RDS.

The Helper instance(s) have read/write access to the shared RDS database but no public-facing services. They only respond to requests from VPN servers, looking up clients in the database and writing back per-client bandwidth consumption information.

The Main, Webhook, Support, Renewer and Admin subsystems have no direct interaction with VPN servers, and therefore no access to client IP addresses or traffic.

All source code and configuration are available to auditors via special-purpose AWS IAM accounts. These accounts also have read access to inspect EC2, RDS, and other AWS systems to fully evaluate the system architecture as deployed.

Evaluation

Based on our investigation of Confirmed's source code and configuration, we believe that no private user information, including IP addresses, is permanently logged to any system or visible to Confirmed staff without tampering visible to auditors. In addition, no private user information is exposed to auditors.

Chain of Trust

Auditors can trust that the code running in production at Confirmed is the same code they are auditing by this chain of trust:

1. EC2 instances are deployed from public, stock Ubuntu AMI
    a. Setup and software installation all auditable from CloudFormation
    b. CodeDeploy for Confirmed's software
2. PROD-Bandwidth code is deployed to VPN servers

    a. *Bandwidth Throttling Script sends clientId, not IP address, to Helper*

3. All deployed code is auditable in AWS CodePipeline, all configuration is auditable in AWS CloudFormation

Any tampering by AWS would be a gross violation of the AWS Terms of Service, and any tampering by Confirmed staff would be visible in CloudTrail and surfaced in Open Watch.

Logs

Logs from production servers are saved to AWS CloudWatch Logs and visible to Confirmed staff. They do not contain private user information, except in special circumstances explained below.

Suricata

Suricata will log the IP addresses of anomalous traffic that matches its rules to `/var/log/suricata/fast.log`, and CloudWatch Logs archives that log stream. This is necessary for Confirmed staff to investigate malicious behavior, and the IP addresses cannot be traced back to client IDs without direct production access. That access would require tampering visible to auditors.

strongSwan

Per `/etc/strongswan.conf`, charon is configured to not log details of VPN connections. Changing this file would be visible to auditors.

Other logs

Per CloudFormation, the only software running on VPN instances is

1) strongSwan charon
2) Suricata
3) Bandwidth script

The bandwidth script is auditable and only sends client IDs to remote systems. The other two are covered above. All other system logs are generic and do not contain any user data.

Database

A single RDS database instance is shared by all subsystems. User email addresses are encrypted at the application layer. Only aggregate bandwidth consumed per user for the most recent month is stored in the database with no history beyond the previous month.

User Data Access

Confirmed staff

Assuming no malicious tampering, Confirmed staff have limited visibility into client activity. They can see logs from production systems, most of which are generic and include no user data. Alerts from Suricata, which include client IP addresses, are persistently logged to CloudWatch for later abuse investigation.

Confirmed staff can access the RDS database only through the Admin and Support subsystems. The raw credentials are stored in SSM Parameter Store, and reading them is logged to CloudTrail and flagged by Open Watch as a violation. The Admin subsystem allows arbitrary SQL queries, but user email addresses are encrypted with a key, also stored in SSM

Parameter Store, and therefore not accessible directly without tampering. Other user data in the database reveals no significant information about a client's location, internet service, or VPN traffic.

Third-party Auditors

Auditors have full read access to most of Confirmed's source code and all of the CloudFormation configuration. They do not have any direct access to production systems, databases, or logs, and this is enforced by AWS IAM.

Potential Attacks

Confirmed employee injects malicious source code
Mitigation**:** Auditors can see every commit in AWS CodeDeploy and will spot the suspicious change.

Confirmed employee tampers with production systems via IAM Roles, SSH, etc.
Mitigation: Open Watch scans CloudTrail logs and flags it as a violation.

Attacker compromises "VPN" instance using 0-day strongSwan exploit
Mitigation: Instances are upgraded at boot and regularly during operation.

Attacker compromises "Main" instance using 0-day Node.js exploit
Mitigation: Main has no direct access to VPN instances, nor IAM permissions to inject code elsewhere in the system. In the worst case, service is degraded and email addresses are revealed to the attacker, but no user traffic or client IP addresses are revealed.

Open Watch

Open Watch is a Mac OS X-native tool, created by Confirmed, to assist auditors in scanning CloudTrail logs for violations of Openly Operated principles. Specifically, it checks for the following events:

- AWS SSM Secret lookup by a human user
  Secrets would allow a Confirmed staff member to decrypt sensitive data.
- AWS IAM Role policy change
  Changes to IAM Roles could grant more permissions to a user than they had at the last audit, invalidating any assertions based on IAM permissions.
- AWS IAM Assume role policy change
  Changes to users' ability to assume IAM roles grant more permissions to a user than they had at the last audit, invalidating any assertions based on IAM permissions.
- AWS SSM SSH Session initiated
  A raw SSH session would allow a Confirmed staff member to tamper with production systems with no visibility to auditors, invalidating any assertions auditors have made about those systems.
- EC2 Key Pair set
  An EC2 instance with a Key Pair set could potentially allow direct SSH access, which would not be visible to auditors.

- EC2 flow logs enabled
  Flow logs would allow a Confirmed staff member to analyze client traffic directly, potentially leaking sensitive user data including IP addresses.
- AWS SSM Run Command
  A command run via SSM allows arbitrary production tampering, invalidating any assertions auditors have made about those systems. The command run is logged to CloudTrail.

This scanning enables auditors to assert that the Confirmed production systems have not been tampered with by anyone, including Confirmed staff.

Without Open Watch, auditors would have a difficult time asserting that no production tampering has taken place. The combination of audit accounts and Open Watch gives auditors strong guarantees that the service is operating as intended.

Feedback

- Open Watch takes 20-40 minutes to download and analyze the current CloudTrail logs as of early December 2018 on a fast internet connection and powerful CPU. The long runtime will discourage auditors from running the tool regularly.
- A (semi-)streaming mode would let auditors monitor CloudTrail logs continuously and respond immediately to violations. Without continuous monitoring, a user must trust nothing malicious has happened since the last run of Open Watch.
- “0 Violations” makes it somewhat difficult for an auditor to trust everything is working as designed. It would be good to have some way for an auditor to see what a violation looks like, even if that’s running the tool against simulated or test-environment CloudTrail logs.

Conclusion

Confirmed VPN’s Openly Operated service protects user privacy and security by isolating private data to hands-off systems and allowing third-party auditors to check for tampering at any time. Based on our investigation of Confirmed’s source code and configuration, we believe that no private user information, including IP addresses, is permanently logged to any system or visible to Confirmed staff without tampering visible to auditors. With a verifiable chain of trust from source code to production systems, Confirmed and its auditors can assert that no user data is viewed by, sold to, or shared with third parties. All source code is visible to auditors, and no code or configuration indicates any exfiltration or leakage of user data. If this were to change, auditors would have immediate visibility into the change and could raise alarms.