Confirmed VPN
Privacy Audit and Open Watch Analysis

Summary Report and Documentation

November 21, 2018

Document Revision History

Version	Modification	Date	Author
1.0	Created Report	Tue, Nov 20, 2018	Ryan Koven

Contacts

Appsec Contacts

Contact	Title	Phone #	Email Address
Ryan Koven	Security Consultant	[hidden]	[hidden]

Application Contacts

Contact	Title	Phone #	Email Address
Johnny Lin	Application Developer		johnny@confirmedvpn.com

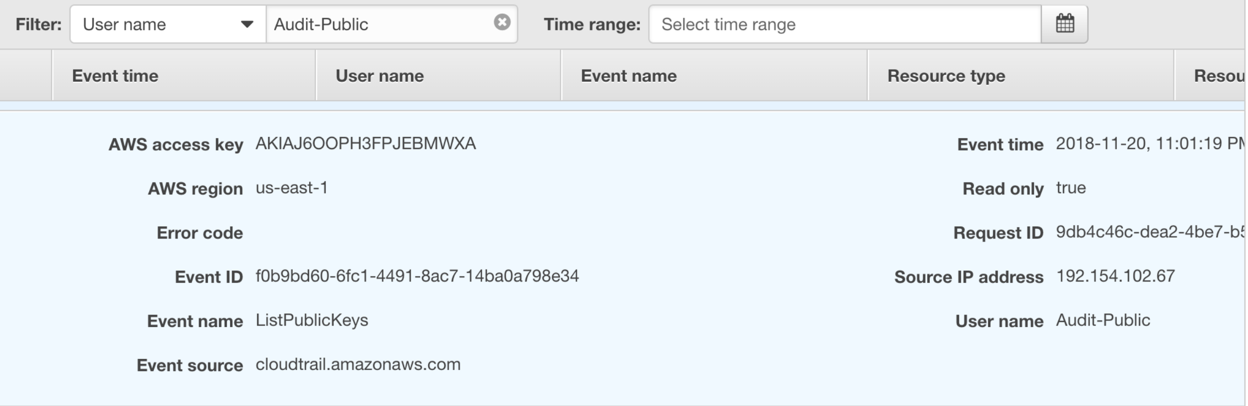
Summary

Confirmed VPN is a subscription VPN service that encrypts users' internet traffic and routes it through secure servers. Confirmed VPN is an open source and "openly operated" service: it intends to allow users to view the source code for the application and to verify the code that is running on application servers. To aid in the verification of its claims as an openly operated service, the Confirmed VPN team built an app called Open Watch that automates several auditing steps that allow users to confirm that claims made by the service are true.

This report summarizes a review of the Open Watch app that included code review and testing to verify functionality. Using a threat model of a malicious service claiming to be openly operated, the review verified that the Open Watch app performs the audit steps it claims to perform, and that the audit steps that the Open Watch app performs provide evidence that Confirmed VPN has not violated any of the basic criteria of an openly operated service. This report may also serve as documentation for auditors who would like to use Open Watch to verify claims made by Confirmed VPN.

Timeframe and Proof of Audit

These activities were performed between 11/20/2018 and 11/21/2018. The audit may be verified by inspecting Cloudtrail logs. The Open Watch app triggers several events that will be logged by Cloudtrail, including the "ListPublicKeys" event as it fetches the public key necessary to verify the signature of the digest file sent with Cloudtrail logs (see screenshot below).



Filter: User name ▾ Audit-Public
Time range: Select time range

Event time	User name	Event name	Resource type	Resou

AWS access key AKIAJ6OOPH3FPJEBMWXA
AWS region us-east-1
Error code
Event ID f0b9bd60-6fc1-4491-8ac7-14ba0a798e34
Event name ListPublicKeys
Event source cloudtrail.amazonaws.com

Event time 2018-11-20, 11:01:19 PM
Read only true
Request ID 9db4c46c-dea2-4be7-b5
Source IP address 192.154.102.67
User name Audit-Public

Confirmed VPN and Open Watch

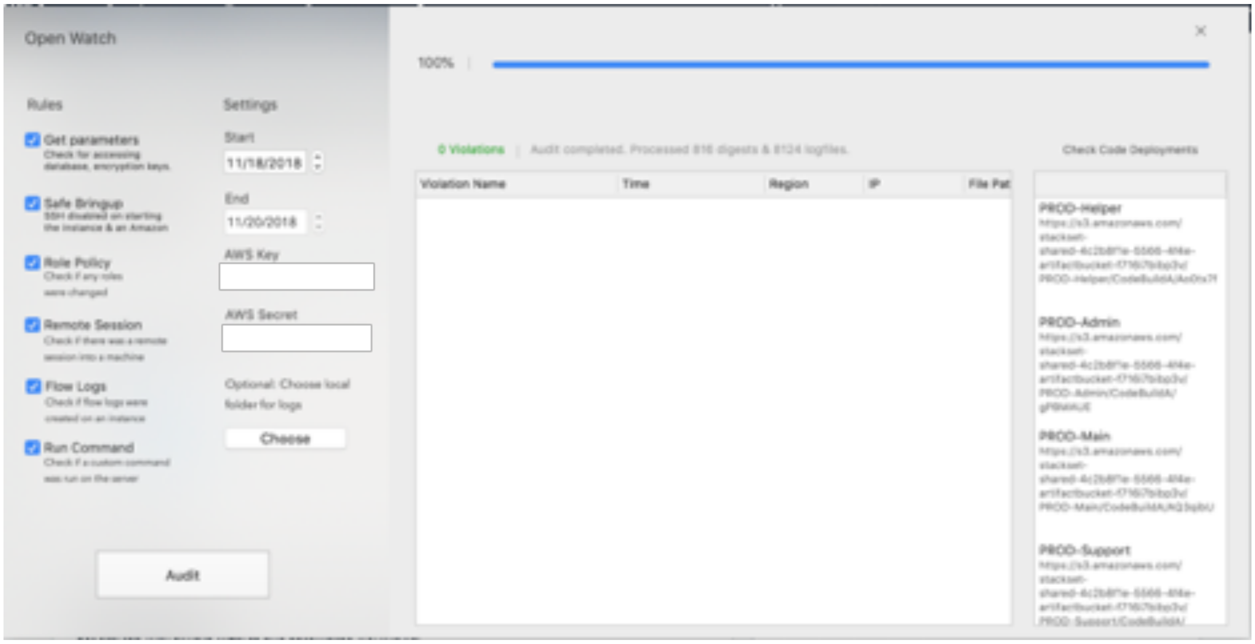
Confirmed VPN uses AWS Cloudtrail to track activity across its AWS infrastructure. The Open Watch app relies on an AWS public audit account to access Cloudtrail logs. Cloudtrail logs contain records of events triggered by AWS APIs, SDKs, command line tools, and management console actions for things like user/role creation, and actions through services like CodeDeploy and CodeCommit. Cloudtrail logs support file integrity validation through SHA-256 hashing and RSA for signing, which helps ensure that logs are authentic and have not been altered.

Confirmed VPN uses CodeCommit to manage source code. The combination of the Cloudtrail logs and CodeCommit repositories make it possible for an auditor to track code deployments and inspect source code running on AWS instances. The state of a repository deployed to AWS instances may be tracked in Cloudtrail logs and viewed in the CodeCommit repository.

Beyond viewing and confirming deployed code, Cloudtrail logs aid auditors in ensuring that operators of a service do not intend to log user data or modify code or data directly on machines. Such an assurance is possible because Cloudtrail logs track events related to AWS roles and policies, remote sessions, logging of data, and creation of parameters for SSH and direct database access, such as key pairs.

Open Watch Audit Details

Open Watch audits sets of rules that form the base of trust for an openly operated service.



Open Watch

Rules

☑ Get parameters
Check for accessing database, encryption keys.

☑ Safe Bringup
SSH disabled on starting the instance & an Amazon

☑ Role Policy
Check if any roles were changed

☑ Remote Session
Check if there was a remote session into a machine

☑ Flow Logs
Check if flow logs were created on an instance

☑ Run Command
Check if a custom command was run on the server

Settings

Start: 11/18/2018

End: 11/20/2018

AWS Key:

AWS Secret:

Optional: Choose local folder for logs

100%

0 Violations | Audit completed. Processed 816 digests & 8124 logfiles.

Violation Name	Time	Region	IP	File Pat

PROD-Helper
https://s3.amazonaws.com/stackset-shared-4c2b8f1e-5566-4f4e-artifactbucket-f7167bibp3v/PROD-Helper/CodeBuildA/Ao0rx7f

PROD-Admin
https://s3.amazonaws.com/stackset-shared-4c2b8f1e-5566-4f4e-artifactbucket-f7167bibp3v/PROD-Admin/CodeBuildA/gF6WAUE

PROD-Main
https://s3.amazonaws.com/stackset-shared-4c2b8f1e-5566-4f4e-artifactbucket-f7167bibp3v/PROD-Main/CodeBuildA/AQ3sjbU

PROD-Support
https://s3.amazonaws.com/stackset-shared-4c2b8f1e-5566-4f4e-artifactbucket-f7167bibp3v/PROD-Support/CodeBuildA/

The app works by downloading Cloudtrail logs from Amazon S3, validating digest files containing log hashes that are signed with the private key of an RSA key pair, and parsing the logs and reporting "rule violations" that represent deviations from the service's openly operated commitment. Open Watch also reports on code deployment events.

Sensitive Parameter Access ("Get Parameters")
Violation: `Secret looked up`

Open Watch looks for evidence of sensitive parameter access in Cloudtrail logs and reports such access as a rule violation. Sensitive parameters include encryption keys that may allow for out-of-band decryption of sensitive data stored in a database.

Direct Access to Machines ("Safe Bringup", "Run Command", "Remote Session")
Violations: `SSH enabled on bringup; SSH session initiated; Run command executed`
Open Watch reports on events from Cloudtrail logs that represent evidence of direct access to machines that may allow operators of the VPN service to alter code, settings, or data on active AWS instances. Events that are evidence of direct access (or the ability for administrators to access machines directly) are logs of remote sessions, a "SendCommand" event for remote commands, logs of SSH sessions, and evidence of SSH access enabled on running instances.

Role Changes ("Role Policy")
Violations: `Role policy change; Assume role policy change`
Role policy changes are tracked and reported by Open Watch. Such changes may be evidence of a service manipulating authentication or access control policies in ways that are not documented or disclosed to users.

Logging of Data ("Flow Logs")
Violation: `Created flow logs`
VPC Flow Logs log information about IP traffic to and from network interfaces in a VPC. Confirmed VPN does not intend to collect data on VPN traffic, so evidence of the creation of Flow Logs is reported by Open Watch as a violation.

Conclusion

Code review and testing confirmed that the Open Watch app performs audit tasks that ensure that Confirmed VPN meets openly operated criteria. During testing, the Open Watch app was used to perform an audit of the Confirmed VPN service, and to track code deployment events in a one-week window. The audit revealed no evidence of violations of openly operated criteria.

No deviations from access control policies verified in an earlier audit were found during this assessment.

The review found no evidence of third-party data sharing or logging of data from internet traffic. As confirmed during the assessment, Cloudtrail logs and CodeCommit repositories allow auditors (perhaps using Open Watch) to verify that the VPN service is not logging or sharing user data. Cloudtrail logs would provide clear evidence of manipulation of application code or servers to log, share, or otherwise exfiltrate user data.