DEMOCRACY LIVE

February 17, 2020

Post Election Security Audit: King Conservation District

DEMOCRACYLIVE
VOTER INFORMATION TECHNOLOGIES

Table of Contents

DEMOCRACYLIVE
VOTER INFORMATION TECHNOLOGIES

Summary

In December 2019, Democracy Live was contracted to provide support for the January 2020 King Conservation District election via its proprietary OmniBallot web application.

OmniBallot has been successfully utilized in hundreds of elections across the country to provide voters the ability to download their ballots on their personal computers, print them out, and mail them to their local election office at their own convenience.

The King Conservation District election was chosen to be a pilot project for a new OmniBallot application: Electronic Ballot Return (EBR). This new application allows voters to complete the entire voting process – including finding their ballot, marking their ballot, and returning their ballot – on their personal device.

Democracy Live considers the safety and integrity of the voting process to be its highest priority, and this is especially true when considering this new ability to return ballots electronically. This document outlines how Democracy Live has verified the integrity of the King Conservation District election. It includes the following:

- A high level overview of the OmniBallot system to provide context.
- An audit of internal facing security measures and procedures used to verify that no Democracy Live employees tampered with voter ballots or return packages.
- An audit of external facing security measures and procedures used to verify that no external actors tampered with voter ballots or return packages.

Distribution

This document is distributed / available to all internal Democracy Live personnel as well as external partners upon request.

Point of Contact

For questions regarding this document or general Democracy Live security issues, please contact the following Democracy Live personnel:

Island Pinnick
Chief Technology Officer
island@democracylive.com

James Johnston
Security Director / Server Administrator / Developer
james@democracylive.com

DEMOCRACYLIVE
VOTER INFORMATION TECHNOLOGIES

OmniBallot Overview

Summary

OmniBallot is an online platform that provides a suite of web applications that can be utilized to deliver balloting information to voters online.

At a high level, OmniBallot consists of the following core components:

- A frontend web application written in Angular JS
- A containerized API written in GoLang
- A MySQL database
- AWS Lambda Functions written in NodeJS

AWS Integration

While the core components of OmniBallot are written and maintained by the Democracy Live development team, this platform is designed to utilize many core a large number of features are provided by Amazon Web Services[1] (AWS).

The AWS services that OmniBallot uses include but is not limited to:

- File storage and static web application hosting via Amazon S3[2]
- Container orchestration and scaling via Amazon Elastic Container Service[3]
- Permissions and Identity handling via AWS Identity and Access Management[4]
- Database hosting and scaling via Amazon Relational Database Service[5]
- Load balancing via Amazon Elastic Load Balancers[6]
- User (County/Jurisdiction) account handling via Amazon Cognito[7]
- Firewall via AWS Web Application Firewall[8]
- Governance, Compliance, and Audit Trails via AWS Cloudtrail[9]
- Application logs, Server logs, and automated alerts via AWS CloudWatch[10]
- Log compilation and aggregation via AWS Athena[11]

[1] https://aws.amazon.com/
[2] https://aws.amazon.com/s3/
[3] https://aws.amazon.com/ecs/
[4] https://aws.amazon.com/iam/
[5] https://aws.amazon.com/rds/
[6] https://aws.amazon.com/elasticloadbalancing/
[7] https://aws.amazon.com/cognito/
[8] https://aws.amazon.com/waf/
[9] https://aws.amazon.com/cloudtrail/
[10] https://aws.amazon.com/cloudwatch/
[11] https://aws.amazon.com/athena/

How Findings were obtained

For most findings contained in this audit, the CloudTrail governance logs for the Democracy Live account were queried using SQL syntax via the AWS Athena service. These queries are provided for the sake of clarity and openness.

Where findings were not obtained via CloudTrail queries, the method will be outlined in the appropriate subsection, to include screenshots or further explanation if necessary.

DEMOCRACYLIVE
VOTER INFORMATION TECHNOLOGIES

Internal Security Audit

Summary

The internal security audit was conducted to identify potential malfeasance on the part of Democracy Live employees. This includes such things as the manipulation, deletion, or download of voter packages or marked ballots.

Threat Vectors

Employees logging into the Root Account and modifying permissions

Summary

This vulnerability involves a Democracy Live employee logging into the root level AWS account and modifying permissions.

Security Implication

Threat level: **Critical**

Many of the restrictions in place to limit potential threats to the integrity of the Electronic Return portion of OmniBallot are contingent on Democracy Live employees not utilizing the root account, as there are no restrictions possible on the root account. An employee accessing the root account could modify permissions, invalidating other security barriers in place.

Security Methods in Place

- Democracy Live has enabled alerts around the use of the Root Account, resulting in a notification being dispatched to the CEO, CTO, and Security Director in the event the root user logs in.

Findings

Classification:	Minor
Methodology:	SELECT * FROM cloudtrail_logs_liveballot_cloudtrail WHERE useridentity.arn = 'arn:aws:iam::468416750693:root' AND eventtime > '2020-01-22T13:00:00Z' AND eventtime < '2020-02-12T04:00:00Z';
Notes:	The root account was accessed on 1/23/2020 in order to delete some files that were generated from King County administrators to test with, as regular user accounts are not allowed to delete EBR files. The root account was accessed on 2/3/2020 in order to update enable premium support with AWS.

Employees downloading voter ballots or packages

Summary

This vulnerability involves a Democracy Live employee accessing a ballot marked by a voter or a package signed by a voter that has been stored in AWS S3 file storage.

Security Implication

Threat level: **High**

An employee downloading a voter ballot or package could result in the loss of voter privacy, thus eroding confidence in the viability of an online voting solution.

Security Methods in Place

- Democracy Live has enabled an IAM policy on all user accounts that disables their ability to download voter ballots or packages.
- This policy has restrictions in place so that it cannot be deleted or modified by normal Democracy Live accounts. Only the root account user can modify this policy.

Findings

Classification:	No Findings
Methodology:	AWS Athena Queries of Cloudtrail Logs: SELECT * FROM cloudtrail_logs_liveballot_cloudtrail WHERE eventtime > '2020-01-22T13:00:00Z' AND eventtime < '2020-02-12T04:00:00Z' AND eventname IN ('DeleteGroupPolicy', 'DeletePolicy', 'DetachGroupPolicy', 'UpdateGroup');
Notes:	Cloudtrail audit found that the IAM restrictions protecting the ballots and packages stored in S3 had not been modified during the period of the King Conservation District election (January 22nd – February 11th). All access to return packages and ballots is logged in an audit log. Review of these audit logs confirmed no Democracy Live employees accessed Electronic Return Resources.

Employees modifying or deleting voter ballots or packages

Summary

This vulnerability involves a Democracy Live employee modifying or deleting a submitted voter ballot or package.

Security Implication

Threat level: **Critical**

An employee modifying or deleting a voter ballot or package could result in fraudulent votes being tallied, resulting in a compromise of the integrity of an election.

Security Methods in Place

- Democracy Live has enabled AWS S3 Object Lock[12] on all voter ballots and packages submitted as part of the Electronic Ballot Return process. Object Lock utilizes a Write Once, Read Many model to ensure that the files have not been modified or deleted.
- In addition, an IAM policy has been implemented that prevents Democracy Live administrator accounts from bypassing the Object Lock restriction (s3:BypassGovernanceRetention). Only the root account user can modify this policy.

Findings

Classification:	No Findings
Methodology:	AWS Athena Queries of Cloudtrail Logs: SELECT * FROM cloudtrail_logs_liveballot_cloudtrail WHERE eventtime > '2020-01-22T13:00:00Z' AND eventtime < '2020-02-12T04:00:00Z' AND eventname IN ('DeleteGroupPolicy', 'DeletePolicy', 'DetachGroupPolicy', 'UpdateGroup');
Notes:	Cloudtrail audit found that the IAM restrictions protecting the ballots and packages stored in S3 had not been modified during the period of the King Conservation District election (January 22nd – February 11th).

[12] https://aws.amazon.com/blogs/storage/protecting-data-with-amazon-s3-object-lock/

Employees modifying CloudTrail audit logs

Summary

This vulnerability involves a Democracy Live employee modifying or deleting the stored audit logs from Amazon Cloudtrail.

Security Implication

Threat level: **High**

Democracy Live utilizes the Amazon CloudTrail service for governance and audit purposes. CloudTrail logs all actions taken in the Omniballot hosting infrastructure. The modification or deletion of any of this data could result in employees being able to commit malicious acts without being detected.

Security Methods in Place

- Democracy Live has enabled an IAM policy around the S3 file storage location where the CloudTrail audit log trails are stored. This policy prevents those files from being modified or deleted by normal Democracy Live developer accounts. Only the root user can modify this policy.
- All log files are stored with CloudTrail Log Integrity [13]enabled. This systems uses industry standard hash functions and public/private key cryptography to provide absolute proof that no log files have been altered or deleted.
- In addition, AWS stores the last 90 days worth of CloudTrail logs by default without creating a trail. This data is held by AWS and can only be read – and not modified – by the user's account.

Findings

Classification:	No Findings
Methodology:	AWS Athena Queries of Cloudtrail Logs: SELECT * FROM cloudtrail_logs_liveballot_cloudtrail WHERE eventtime > '2020-01-22T13:00:00Z' AND eventtime < '2020-02-12T04:00:00Z' AND eventname IN ('DeleteGroupPolicy', 'DeletePolicy', 'DetachGroupPolicy', 'UpdateGroup');
Notes:	A review of the last 90 days (undertaken on 2/24/2020) of immutable logs from AWS shows no modifications to objects contained within the CloudTrail storage bucket. An audit of the CloudTrail logs shows no modification of the IAM policy preventing write access to the stored log location.

[13] https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-log-file-validation-intro.html

DEMOCRACYLIVE
VOTER INFORMATION TECHNOLOGIES

External Security Audit

Summary

The external security audit was conducted to identify potential breaches in the OmniBallot application or underlying AWS infrastructure by outside actors.

Threat Vectors

AWS Account Compromise

Summary

This vulnerability involves an outside attacker gaining access to the AWS cloud account or security credentials of a Democracy Live developer and logging into the AWS console or accessing resources via the AWS CLI.

Security Implication

Threat level: **Critical**

Democracy Live developers have elevated privileges and nearly unlimited access to all resources hosted in AWS. The loss or compromise of developer credentials could result in major loss of OmniBallot functionality or customer data.

Security Methods in Place

- AWS GuardDuty generates findings whenever a console login or credential use occurs from a new or unusual IP address. Any findings of this nature are immediately dispatched to the Democracy Live Security Director.
- Democracy Live developers are required to rotate their passwords and access keys at least every 90 days.
- AWS Cloudtrail provides a permanent audit log of all account logins and credential use.

Findings

Classification:	No Findings
Methodology:	AWS Athena Queries of Cloudtrail Logs: SELECT * FROM cloudtrail_logs_liveballot_cloudtrail WHERE eventname = 'CreateAccessKey' AND eventtime > '2020-01-22T00:00:00Z' AND eventtime < '2020-02-12T00:00:00Z'; SELECT * FROM cloudtrail_logs_liveballot_cloudtrail

	WHERE eventname = 'CreateUser' AND eventtime > '2020-01-22T00:00:00Z' AND eventtime < '2020-02-12T00:00:00Z';
Notes:	GuardDuty observed no unusual sign in attempts from Democracy Live accounts for the period of the King Conservation District election (January 22nd – February 11th) Cloudtrail audit found no new/unexpected accounts or credentials had been created for the applicable election period.

DEMOCRACYLIVE
VOTER INFORMATION TECHNOLOGIES

OmniBallot application disabled via Denial of Service (DOS/DDOS) attack

Summary

This vulnerability involves an attacker flooding the OmniBallot API or database with HTTP requests, resulting in excessive load and potential downtime.

Security Implication

Threat level: **High**

Any unexpected downtime in the OmniBallot application could prevent voters from accessing the system and submitting their ballots.

Security Methods in Place

- Democracy Live utilizes the AWS Web Application Firewall service to help guard against DOS/DDOS style attacks. This firewall utilizes a rate limit of 100 HTTP requests per 5 minutes per IP address and upon violation of that threshold adds the given address to a blacklist.
- Upon a given IP address violating that threshold, an alert is immediately dispatched to Democracy Live personnel for investigation.
- The OmniBallot API is configured to scale with demand to help mitigate the threat of downtime.

Findings

Classification:	Minor
Methodology:	AWS Athena Queries of Cloudtrail Logs: SELECT * FROM apifirewalllogs WHERE timestamp > 1579651666000 AND timestamp < 1581466066000 AND terminatingruleid = 'b88bc58c-c597-446b-8976-92133df28319’;
Notes:	On February 10th, an alert was dispatched to the Democracy Live Security Director that an IP address had violated the rate limit threshold and had been added to the blacklist. Upon investigation, it was revealed that the IP address had originated in China and that they were attempting to fish for various configuration files (php.info, admin/login portals, etc). This was no threat to the OmniBallot system and resulted in no downtime or data loss.

DEMOCRACYLIVE
VOTER INFORMATION TECHNOLOGIES

OmniBallot data compromised via a SQL Injection Attack

Summary

This vulnerability involves an attacker attempting to run malicious SQL commands against the OmniBallot API or database, resulting in data loss or compromise.

Security Implication

Threat level: **High**

The loss or compromise of data via a successful SQL injection attack could result in data loss or manipulation.

Security Methods in Place

- Democracy Live utilizes the AWS Web Application Firewall service to help guard against SQL Injection attacks. This firewall utilizes a filter that decodes the request headers, body, URI, query string, and cookies and evaluates the result to match potential SQL injection threats.
- The OmniBallot API also utilizes libraries to strip special characters out of potential queries.

Findings

Classification:	Minor
Methodology:	AWS Athena Queries of Cloudtrail Logs: SELECT * FROM apifirewalllogs WHERE timestamp > 1579651666000 AND timestamp < 1581466066000 AND terminatingruleid = '033bbcda-8fb5-4ec8-97f4-fcb342111e9d';
Notes:	Over the course of the King County Conservation District election period, there were 123 requests evaluated that resulted in a finding of a SQL injection threat. All of these requests were blocked before reaching the OmniBallot API. No data was lost and no system was compromised by these attempts.

DEMOCRACYLIVE
VOTER INFORMATION TECHNOLOGIES

King County Administrator account compromise

Summary

This vulnerability involves an attacker gaining access to the administrative account of a King Conservation District administrator.

Security Implication

Threat level: **Critical**

Account administrators have elevated privileges, including the ability to modify ballot data, voter records, and EBR submissions. A compromise of their account could result in all ballots cast in an election rendered unusable or invalid.

Security Methods in Place

- All Administrative accounts are required to meet password complexity requirements that prevent attacks from being able to easily brute force accounts via known password crack lists.
- Democracy Live monitors and logs all logins to the administrative portal. These logins are categorized as either low, medium, or high risk based upon such factors as logging in to the portal from a new, unrecognized device or an unusual IP address.

Findings

Classification:	Minor
Methodology:	The Democracy Live Chief Technical Officer ran a script that extracted the login histories of all KCD administrator accounts to review all signins, flagging any that were not 'low' risk. This script can be made available upon request.
Notes:	• No accounts were automatically blocked from login • No logins were categorized as "High" risk. • One login was categorized as "Medium" risk. This was a known instance of an administrator logging in from her home account.