Mobile Apps Exposing AWS Keys Affect 100M+ Users' Data

CloudSEK

0.5% of Mobile Apps on the Internet Expose AWS API Keys

Amazon Web Services (AWS) is the preferred cloud computing platform for enterprises, small businesses, and even governments worldwide. From NASA to Netflix, AWS services and APIs are used by millions of companies for their infrastructure needs, hosting requirements, and to enable their websites and mobile apps. This is why threat actors are constantly looking for ways to compromise a company's AWS services to get their hands on sensitive information, user data, and internal networks.

CloudSEK's BeVigil, a security search engine for mobile apps, has found that 0.5% of mobile apps expose AWS API keys, thus putting their internal networks and data at high risk.

Critical Flaw in How Mobile App Developers Use AWS

APIs have revolutionized how apps are developed and used. They make it easy for developers to build apps that communicate with multiple sources and efficiently manage data flowing to and from the apps. In the case of AWS, the API acts like a password for the app to access data stored on AWS. In simple words, if AWS is your apartment, where you store critical data and files, the API key unlocks your front door.

While public API keys, such as that of Facebook and LinkedIn, are intentionally made available for other apps to verify user identities, most apps use private keys that need to be kept secure. However, given the pace at which new versions of apps are released, and the fast pace at which developers work, it is not uncommon for developers to overlook exposed API keys.

CloudSEK has observed that a wide range of companies — both large and small — that cater to millions of users have mobile apps with API keys that are hardcoded in the app packages.

These keys could be easily discovered by malicious hackers or competitors who could use it to compromise their data and networks. In fact, multiple recent high-profile hacks, such as the Imperva breach, have leveraged this misconfiguration to compromise cloud infrastructure. Hence, hardcoded API keys are akin to locking your house but leaving the key in an envelope titled “do not open.”

While this is not a flaw in AWS, it is evidence of how sloppily AWS keys are handled. So, it is up to individual companies to address the security concerns associated with using AWS services.

Identifying Mobile Apps Exposing AWS API Keys

Despite having over 8 million apps to choose from, users, app developers, and security researchers don’t have a mechanism to determine the security posture of mobile apps. To address this gap, CloudSEK launched BeVigil — the world’s first security search engineer for mobile apps, in April 2021.

Given how time-consuming and expensive security reviews can be, developers often skip this step before apps are shipped off to various app stores. And it doesn’t help that end users don’t have any mechanisms to ensure that the apps they install are secure. This leads to user data being breached and then sold on underground forums to the highest bidder. But with BeVigil, users can now ascertain the risk rating of an app, check the list of permissions it requests, and ensure it is not malicious. Moreover, app developers can proactively upload their apps to BeVigil to identify vulnerabilities and remediate them, avoiding any pitfalls before their launch. In addition, security researchers can perform in-depth investigations on millions of apps using their metadata and by searching the app packages for code snippets, keywords, strings, or other expressions that denote vulnerabilities. And the scan reports generated by BeVigil are made available to the global CloudSEK community.

Analysis of 10,000 Apps

In the past month, over 10,000 apps have been uploaded to BeVigil for analysis. Out of which, we found 40+ apps, i.e 0.5% of the apps, had hardcoded private AWS keys. And in total, the 40+ apps have more than 100 million downloads. Given that there are over 8 million apps available across app stores, we estimate that there are thousands of mobile apps exposing

AWS keys. With many of these apps catering to millions of users, there needs to be widespread awareness about the risks involved.

CloudSEK has responsibly disclosed these security concerns to AWS and the affected companies independently.
Listing some of the popular apps that were exposing private AWS keys. For security reasons we are only listing apps whose keys are deactivated.

Organisation	App ID	No. of Installs	Category	Country
Clubfactory	club.fromfactory	100,000,000+	Ecommerce	India
Adobe Photoshopfix	com.adobe.adobephotoshopfix	10,000,000	Photography	United States
Adobe Comp	com.adobe.comp	500,000+	Art & Design	United States
Weather Forecast & Snow Radar	com.weather.weather	100,000,000	Weather	United States
Wholee - Online Shopping Store	com.wholee	1,000,000	Shopping	Singapore
Oven Story Pizza	in.ovenstory	1,000,000	Food & Drink	India
Hootsuite:	com.hootsuite.droid.full	5,000,000	Social	Canada

Impact of Leaked AWS Keys

AWS keys hardcoded in a mobile app source code can be a huge problem especially if it's IAM role has wide scope and permissions. The possibilities for misuse are endless here, since the attacks can be chained, and the attacker can gain further access to the whole infrastructure, even the codebase and config.

Let's look at the example of a PlayStore app with half a million downloads to understand the impact.

As seen below, this app has a hardcoded AWS key and secret in it's strings.xml file:

```
183     <string name="allText">ALL</string>
184     <string name="all_notification">All Notifications</string>
185     <string name="all_scores">All Scores</string>
186     <string name="all_scoresBtnTxt">All Scores</string>
187     <string name="amezon_app_id">AKIA[redacted]JA</string>
188     <string name="amezon_app_key">Yxwz[redacted]rLg5W</string>
```

This key has access to multiple AWS services including **ACM (Certificate Manager), ElasticBeanstalk, Kinesis, OpsWorks, and S3.** We focused on the S3 access to understand the extent of the risk. We found that the AWS credentials have access to 88 S3 buckets (read/write) which **collectively contain 10,073,444 files that amount to a total of 5.5 terabytes of data.**

These buckets were deployed to host files and data generated from various projects. We found **application source code, backup files, user reports, test artifacts, user uploads, logs, wordpress backup, user certificates, config files, credential files,** and more, distributed across these buckets.

From the application backups, and config files, one can obtain more credentials such as database hostnames, passwords, tokens and gain further access to the underlying infrastructure.

Here is the database Config file that contains plain text password to mysql:

```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', '[redacted]

/** MySQL database username */
define('DB_USER', '[redacted];

/** MySQL database password */
define('DB_PASSWORD', '[redacted]

/** MySQL hostname */
define('DB_HOST', 'oustlabsdb.[redacted]amazonaws.com:3306');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8mb4');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');
```

The following database can be accessed using the password:

Sr.Num	UserId	Ful	Groups	Register Date	First Login	Last Seen Date	Total Learning Time
1	C0(:om	Arv ɔa	Mumbai & Pune	2020-04-23	2020-04-29	2020-04-29	56s
2	C0(:om	Sid ıok	Mumbai & Pune	2020-04-23	2020-04-29	2020-04-29	2m 22s
3	C0(:om	Kur	Mumbai & Pune	2020-04-23	2020-04-29	2020-04-29	8m 36s
4	DG i.com	B A .	Hyderabad	2020-04-09	2020-04-29	2020-04-29	5m 23s
5	DG i.com	Ma ːh	Hub Manager	2020-04-09	2020-04-29	2020-04-29	17m 8s
6	C0(:om	Sat	Mumbai & Pune	2020-04-23	2020-04-29	2020-04-29	18m
7	C0(:om	Bor ti Vinod Kumar	Hyderabad	2020-04-09	2020-04-29	2020-04-29	21m 6s
8	DG i.com	Ont ĸarao	Hyderabad	2020-04-09	2020-04-29	2020-04-29	27m 37s
9	DG i.com	Dur	Hyderabad	2020-04-29	2020-04-29	2020-04-29	16m 17s
10	C0(:om	Tus	Mumbai & Pune	2020-04-23	2020-04-29	2020-04-29	6m 18s
11	C0(:om	Pra ɓoud	Hyderabad	2020-04-29	2020-04-29	2020-04-29	23m 47s
12	DG i.com	Sag	Hub Manager	2020-04-23	2020-04-29	2020-04-29	19s
13	DG i.com	Asi	Mumbai & Pune	2020-04-23	2020-04-29	2020-04-29	2m 23s
14	DG i.com	Fai ı	Hub Manager	2020-04-23	2020-04-29	2020-04-29	11m 11s
15	DG i.com	Ma Cheemala	Hyderabad	2020-04-29	2020-04-29	2020-04-29	17m 3s
16	DG i.com	Sat	NCR	2020-04-23	2020-04-29	2020-04-29	43s
17	DG i.com	Yas M	Bangalore	2020-04-28	2020-04-29	2020-04-29	1m 48s
18	DG i.com	Shi - H V	Bangalore	2020-04-28	2020-04-29	2020-04-29	1m 14s
19	DG i.com	Mo ːer Khan	Hyderabad	2020-04-09	2020-04-29	2020-04-29	24m 7s
20	DG i.com	Gaj Prem Kumar	Hyderabad	2020-04-09	2020-04-29	2020-04-29	25m 28s
21	DG i.com	Gor ar .	Hyderabad	2020-04-09	2020-04-29	2020-04-29	10m 16s
22	DG i.com	Kis nt	Mumbai & Pune	2020-04-23	2020-04-29	2020-04-29	0 ms
23	DG i.com	Ray	NCR	2020-04-29	2020-04-29	2020-04-29	19m 35s
24	DG i.com	Thc een	Hyderabad	2020-04-09	2020-04-29	2020-04-29	9s
25	kar kar		null	2020-04-21	2020-04-29	2020-04-29	22m 17s
26	C0(:om	Ma si .	Hyderabad	2020-04-09	2020-04-29	2020-04-29	19m 53s
27	C0(:om	Mu hil Reddy	Hyderabad	2020-04-09	2020-04-29	2020-04-29	10m 28s
28	DG i.com	Ach ishna	Hyderabad	2020-04-09	2020-04-29	2020-04-29	16m 55s
29	C0(:om	Hyc ı	Hyderabad	2020-04-29	2020-04-29	2020-04-29	10m 56s
30	DG i.com	Azr ɜn	Hyderabad	2020-04-29	2020-04-29	2020-04-29	36m 50s
31	DG i.com	Pitl ar	Hyderabad	2020-04-09	2020-04-29	2020-04-29	22m 24s
32	DG i.com	Boy r	Hyderabad	2020-04-09	2020-04-29	2020-04-29	30m 32s
33	DG i.com	Nav nar	Hyderabad	2020-04-29	2020-04-29	2020-04-29	21m 13s
34	DG i.com	A. ı dy	Hyderabad	2020-04-29	2020-04-29	2020-04-29	26m 5s
35	C0(:om	Nac ɜai Kumar	Hyderabad	2020-04-09	2020-04-29	2020-04-29	34m 36s
36	DG i.com	Naj ra SK	Hyderabad	2020-04-29	2020-04-29	2020-04-29	28m 52s

Threat Actors are Continuously Scanning for Exposed AWS Keys

CloudSEK Threat Intel researchers have observed several high-profile threat actors scanning for and selling AWS keys, access to S3 buckets, and databases obtained by exploiting exposed AWS keys.

Some high-profile hacks that leveraged exposed AWS Keys:

Target	Date	Impacted Assets
Upstox	April 2021	Hacker group ShinyHunters leaked 2.5 million users' data and 56 million Know Your Customer (KYC) data. Multiple other high profile hacks by ShinyHunters have used the same technique of using AWS keys from leaked source codes, mobile apps, etc.

Fresh Films	January 2020	PII including names, postal and email addresses, phone numbers, birth dates and bank details, as well as passport scans and the National Insurance numbers.
Accenture	October 2017	40k passwords, tech info, API keys etc.
Dow Jones & Company	July 2017	Sensitive personal and financial details of ~2 million customers
Verizon	July 2017	Personal data of 14 million Verizon customers
WWE	July 2017	Personal information of 3 million customers
Uber	October 2016	Personal information of 57 million users worldwide, including 600,000 U.S. drivers.

Responsible Use of AWS Keys

When you use AWS programmatically, you provide your AWS access keys so that AWS can verify your identity in programmatic calls. Your access keys consist of an access key ID (for example, AKIAIOSFODNN7EXAMPLE) and a secret access key (for example, wJalrXUtnFEMI/K7MDENG/ bPxRfiCYEXAMPLEKEY). Anyone who has your access keys has the same level of access to your AWS resources as you do.

Refer to AWS documentation on how to access your resources with your keys securely. The fundamental security practice is to not hardcode them anywhere.

What to Do If You Inadvertently Expose an AWS Access Key?

If your AWS Key has been inadvertently exposed you can revoke or delete the access key by following the steps mentioned here.

About CloudSEK

CloudSEK is an AI-driven Digital Risk Management Enterprise. CloudSEK's XVigil platform helps clients assess their security posture in real-time from the perspective of an attacker. XVigil scours thousands of sources (across the surface, deep and dark web), to detect cyber threats, data leaks, brand threats, identity thefts, etc. To learn more about how the CloudSEK XVigil platform can strengthen your external security posture and deliver value from Day 1, visit https://cloudsek.com/ or drop a note to sales@cloudsek.com