



모듈 프로젝트 최종 발표

루키즈 9기 김태진

22.10.14





주제 소개

CVE 통합 검색 사이트

취약점 검색 시 여러 사이트를 이용해야 하는 불편함 해소.
Exploit-db, Cve.mitre, KISA, Google

새로운 취약점이 등장하거나 침해 사고 발생 시 접속량
증가를 예방하기 위한 **로드 밸런싱과 오토 스케일링 적용.**

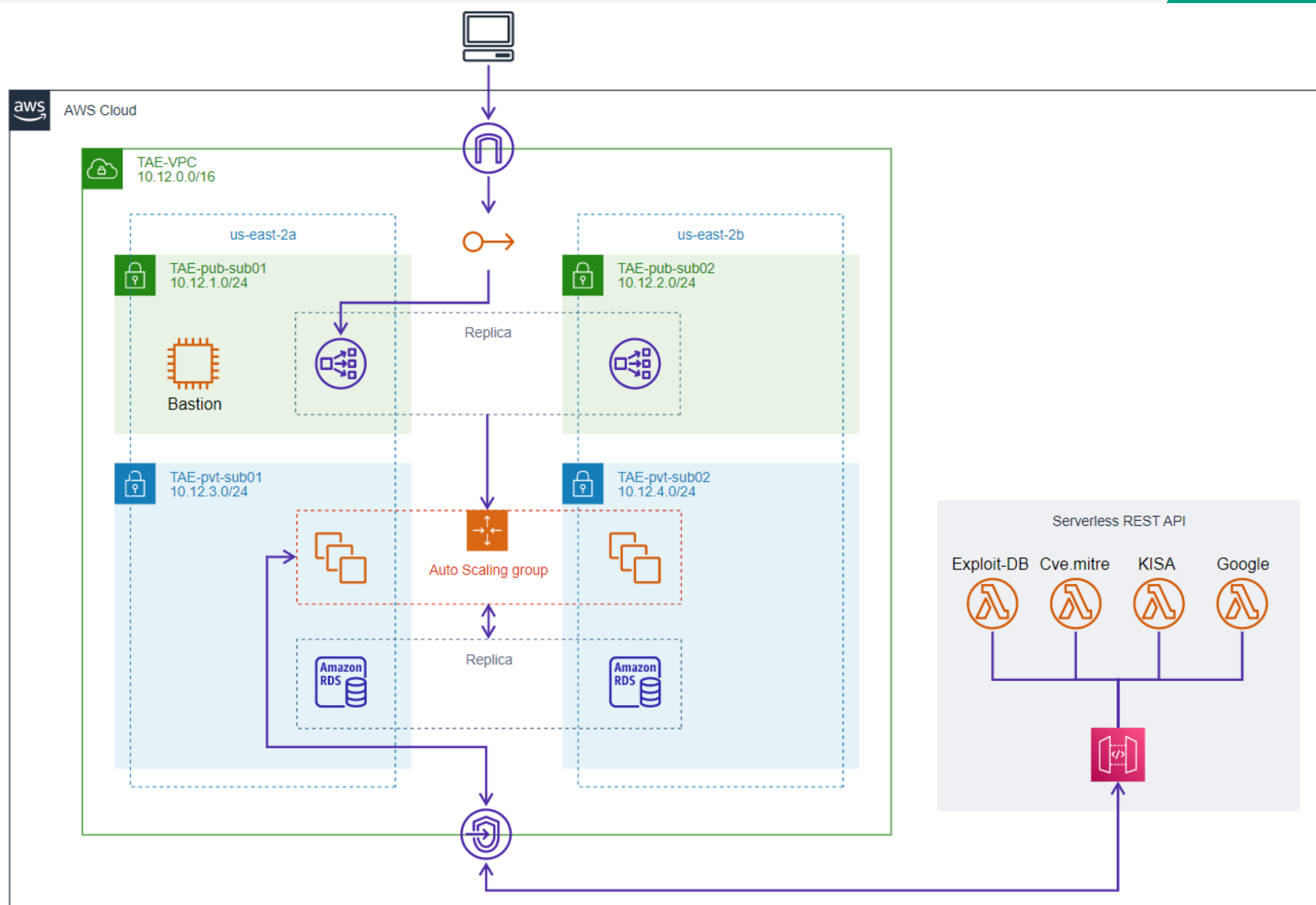
Lambda + API Gateway + VPC End point를 적용한
프라이빗 API를 구현하여 기능의 분산과 서버의 부하 감소.

각 사이트의 검색 결과를 크롤링을 통해 종합한 **통합 검색.**
회원 시스템으로 유저 별 **키워드 저장 기능** 제공.





AWS Architecture





AWS Config

서브넷 (4) 정보

Q 서브넷 필터링

<input type="checkbox"/>	Name ▾	서브넷 ID ▾	상태 ▾	VPC ▾	IPv4 CIDR ▾	IPv... ▾	사용... ▾	가용 영역 ▾	가용 영역 ID ▾
<input type="checkbox"/>	TAE-pvt-sub02	subnet-0d2540e4053c9c5af	✔ Available	vpc-06...	10.12.4.0/24	-	249	us-east-2b	use2-az2
<input type="checkbox"/>	TAE-pub-sub02	subnet-0e710e375caa6c546	✔ Available	vpc-06...	10.12.2.0/24	-	250	us-east-2b	use2-az2
<input type="checkbox"/>	TAE-pvt-sub01	subnet-079a3df679c0d0137	✔ Available	vpc-06...	10.12.3.0/24	-	248	us-east-2a	use2-az1
<input type="checkbox"/>	TAE-pub-sub01	subnet-0eabd47b7b42b2dad	✔ Available	vpc-06...	10.12.1.0/24	-	248	us-east-2a	use2-az1

라우팅 테이블 (2) 정보

Q 라우팅 테이블 필터링

<input type="checkbox"/>	Name ▾	라우팅 테이블 ID ▾	명시적 서브넷 연결
<input type="checkbox"/>	pvt-rt	rtb-031bfbb7d0fb0df2e	2 서브넷
<input type="checkbox"/>	pub-rt	rtb-00ea199ae1409cda1	2 서브넷

라우팅 (2)

라우팅 편집

Q 라우팅 필터링

모두 ▾

< 1 > ⚙

대상 ▾	대상 ▾	상태 ▾	전파됨 ▾
0.0.0.0/0	igw-0296809c8f94f8e3a	✔ 활성화	아니요
10.12.0.0/16	local	✔ 활성화	아니요

VPC 설정

- Public subnet, Private subnet를 가용 영역 당 한 개씩 구성
- public subnet과 private subnet은 각 라우팅 테이블을 가지며 public 라우팅 테이블만 인터넷에 연결



AWS Config

로드 밸런서: TAE-nlb

설명 리스너 모니터링 통합 서비스 태그

기본 구성

이름	TAE-nlb
ARN	arn:aws:elasticloadbalancing:us-east-2:373536100836:loadbalancer/net/TAE-nlb/70899ac8f116b5bc 🔗
DNS 이름	TAE-nlb-70899ac8f116b5bc.elb.us-east-2.amazonaws.com 🔗 (A 레코드)
상태	활성
유형	network
체계	internet-facing
IP 주소 유형	ipv4 IP 주소 유형 편집
VPC	vpc-06ebdcc366d35f277 🔗
가용 영역	subnet-0eabd47b7b42b2dad - us-east-2a 🔗 IPv4 주소: 탄력적 IP 3 🔗 subnet-0e710e375caa6c546 - us-east-2b 🔗 IPv4 주소: AWS에서 할당 서브넷 편집
호스팅 영역	ZLMOA37VPKANP
생성 시간	2022년 10월 13일 오후 11시 57분 57초 UTC+9

Network Load balancer

- Internet-facing을 위해 Public subnet에 배치하고 두 개의 가용 영역을 사용하여 가용성 향상
- EIP 할당을 통한 정적 주소로 Private subnet의 AutoScaling Group을 연결함
- L7계층인 alb보다 속도가 빠르고 더 향상된 부하 분산 방식을 제공



AWS Config

그룹 세부 정보

[편집](#)

원하는 용량
2

최소 용량
1

최대 용량
3

Auto Scaling 그룹 이름
TAE-AS

생성된 날짜
Fri Oct 14 2022 00:01:21 GMT+0900 (한국 표준 시)

Amazon 리소스 이름(ARN)
arn:aws:autoscaling:us-east-2:373536100836:autoScalingGroup:08e4a8c6-32bc-4a4c-bf6b-e1575db4df1c:autoScalingGroupName/TAE-AS

시작 구성

[편집](#)

시작 구성
TAE_LC

AMI ID
ami-0d20839558f5d1b41

인스턴스 유형
t2.micro

키 페어 이름
CVE_key

스토리지(블륨)
/dev/sda1

[시작 구성 콘솔에서 세부 정보 보기](#)

보안 그룹
[sg-02338f5526f751fc1](#)

생성 시간
Thu Oct 13 2022 23:59:30 GMT+0900 (한국 표준 시)

인바운드 규칙 (3)

[태그 관리](#)[인바운드 규칙 편집](#)

1



<input type="checkbox"/>	Name ▾	보안 그룹 규칙 ID ▾	IP 버전 ▾	유형 ▾	프로토콜 ▾	포트 범위 ▾	소스 ▾	설정
<input type="checkbox"/>	-	sgr-044a0a04cb10a64fd	IPv4	SSH	TCP	22	10.12.1.115/32	-
<input type="checkbox"/>	-	sgr-08daba36ce559a528	IPv4	HTTP	TCP	80	0.0.0.0/0	-
<input type="checkbox"/>	-	sgr-07f8276f52d21b5be	IPv4	HTTPS	TCP	443	0.0.0.0/0	-

Auto Scaling

- Public에 Image host를 이용하여 AMI 생성
- Private에 타겟 그룹 설정 후 Auto Scaling 생성
- 생성되는 EC2의 내부는 보안 그룹과 SSH 키를 이용해 배스천에서만 SSH로 연결 가능하도록 설정



AWS Config

pvt-sng

서브넷 그룹 세부 정보

VPC ID
vpc-06ebdcc366d35f277

ARN
arn:aws:rds:us-east-2:373536100836:subgrp:pvt-sng

지원되는 네트워크 유형
IPv4

설명
pvt-sng

서브넷 (2)

가용 영역	서브넷 ID	CIDR 블록
us-east-2b	subnet-0d2540e4053c9c5af	10.12.4.0/24
us-east-2a	subnet-079a3df679c0d0137	10.12.3.0/24

보안 그룹 규칙 (4)

보안 그룹 규칙을(를) 기준으로 필터링

보안 그룹	유형	규칙
rds-sg (sg-09ab8ea30ba972fed)	CIDR/IP - Inbound	10.12.3.0/24
rds-sg (sg-09ab8ea30ba972fed)	CIDR/IP - Inbound	10.12.4.0/24
rds-sg (sg-09ab8ea30ba972fed)	CIDR/IP - Inbound	10.12.1.115/32
rds-sg (sg-09ab8ea30ba972fed)	CIDR/IP - Outbound	0.0.0.0/0

```
mysql> select host, user from user;
+-----+-----+
| host      | user      |
+-----+-----+
| %         | admin     |
| 10.12.%   | searcher  |
| 10.12.1.115 | bastion   |
| localhost | mysql.infoschema |
| localhost | mysql.session |
| localhost | mysql.sys  |
| localhost | rdsadmin   |
+-----+-----+
7 rows in set (0.00 sec)
```

RDS

- Private 서브넷 그룹을 설정하여 Private 배치
- 보안 그룹 설정으로 private subnet과 bastion Host에서만 접근 가능
- mysql 내에서 bastion Host만 사용 가능한 계정과 웹 서버에서 사용하는 계정을 네트워크로 제한



AWS Config

```
ubuntu@ip-10-12-1-115:~$ ssh -i "CVE_key.pem" ubuntu@10.12.3.73
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-1019-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Thu Oct 13 16:38:22 UTC 2022

System load:  0.0               Processes:            112
Usage of /:   22.5% of 7.57GB   Users logged in:     0
Memory usage: 23%              IPv4 address for eth0: 10.12.3.73
Swap usage:   0%

46 updates can be applied immediately.
19 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Last login: Thu Oct 13 14:41:48 2022 from 123.214.11.232
ubuntu@ip-10-12-3-73:~$
```

인바운드 규칙 (1/1)

Q 보안 그룹 규칙 필터

<input checked="" type="checkbox"/>	Name ▾	보안 그룹 규칙 ID ▾	IP 버전 ▾	유형 ▾	프로토콜 ▾	포트 범위 ▾	소스 ▾
<input checked="" type="checkbox"/>	-	sgr-04ac889a1a13...	IPv4	SSH	TCP	22	123.214.11.232/32

```
ubuntu@ip-10-12-1-115:~$ mysql -h tae-db.czdlwojwx0j.us-east-2.rds.amazonaws.com -u bastion -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 128
Server version: 8.0.28 Source distribution

Copyright (c) 2000, 2022, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

Bastion Host

- SSH만 접근 허용하여 비밀 키로만 접근 가능
- 배스천 키와 다른 비밀 키를 이용해 배스천에서만 private EC2에 접근 가능
- RDS 관리 계정으로 접근 가능



AWS Config

Lambda > 함수

함수 (4)

태그 및 속성별 필터

☐ 함수 이름

☐ kisa

☐ google

☐ exploitdb

☐ cvemitre

```
lambda_function x Execution results x
2 import requests
3 from bs4 import BeautifulSoup as bs
4
5
6 def lambda_handler(event, context):
7     ret = []
8     keyword = event['keyword']
9
10    param = {
11        'q': keyword,
12        'draw': 1
13    }
14    header = {
15        'accept': 'application/json, text/javascript, */*; q=0.01',
16        # 'sec-fetch-dest': 'empty',
17        # 'sec-fetch-mode': 'cors',
18        'x-requested-with': 'XMLHttpRequest'
19    }
20    req = requests.get(
21        'https://www.exploit-db.com/search',
22        params=param,
23        headers=header
24    )
25
26    data = json.loads(req.text)
27    for i in data['data']:
28        dic = {}
29        dic['title'] = i['description'][1]
30        dic['url'] = f"https://www.exploit-db.com/exploits/{i['id']}"
31        dic['code'] = [ f"{j['code_type']}-{j['code']}" for j in i['code']]
32        ret.append(dic)
33
34    # TODO implement
35    return {
36        'statusCode': 200,
37        'body': json.dumps(ret)
38    }
```

Response

```
{
  "statusCode": 200,
  "body": [
    {
      "title": "Samba 2.2.x - Remote Buffer Overflow",
      "url": "https://www.exploit-db.com/exploits/7",
      "code": [
        "osvdb-4469",
        "cve-2003-0201"
      ]
    },
    {
      "title": "Samba & 2.2.8 (Linux/BSD) - Remote Code Execution",
      "url": "https://www.exploit-db.com/exploits/10",
      "code": [
        "osvdb-4469",
        "cve-2003-0201"
      ]
    },
    {
      "title": "Samba 2.2.8 - Brute Force Method Remote Command Execution",
      "url": "https://www.exploit-db.com/exploits/55",
      "code": [
        "osvdb-4469",
        "cve-2003-0201"
      ]
    },
    {
      "title": "Microsoft Windows XP/2003 - Samba Share Resource Exhaustion (Denial of Service)",
      "url": "https://www.exploit-db.com/exploits/148",
      "code": [
        "osvdb-60587"
      ]
    }
  ]
}
```

Lambda

- 각 사이트에 해당하는 파이썬 크롤링 코드를 적용하여 정보를 수집
- Lambda에 키워드 요청 시 Json형식의 데이터를 출력



AWS Config

리소스

- /
- /cvemitre
POST
- /exploitdb
POST
- /google
POST
- /kisa
POST

엔드포인트 (1/1) 정보

엔드포인트 필터링

Name	VPC 엔드포인트 ID	VPC ID	서비스 이름
TAE-ep	vpce-00d0319a3c903458a	vpc-06ebdcc366d35f277 TAE-vpc	com.amazonaws.t

vpce-00d0319a3c903458a / TAE-ep

세부 정보 | **서브넷** | 보안 그룹 | 알림 | 정책 | 모니터링 | 태그

서브넷 (2)

서브넷 필터링

서브넷 ID	가용 영역	IPv4 주소
subnet-0d2540e4053c9c5af (TAE-pvt-...	us-east-2b (use2-az2)	10.12.4.81
subnet-079a3df679c0d0137 (TAE-pvt-...	us-east-2a (use2-az1)	10.12.3.160

리소스 정책

리소스 정책을 사용하여 이 프라이빗 API에 액세스 제어를 구성합니다. 액세스는 AWS 계정, 소스 VPC 부여 유형을 사용할 수 있습니다. 보안 주체가 AWS로 설정된 경우, 보안이 되지 않은 리소스를 포함해

중요

특정 VPC 및 VPC 엔드포인트에 대한 액세스를 제한하려면 API의 리소스 정책에 'aws:SourceVpc' 및

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Deny",  
6       "Principal": "*",  
7       "Action": "execute-api:Invoke",  
8       "Resource": "arn:aws:execute-api:us-east-2:373536100836:006bq9bckd/*",  
9       "Condition": {  
10        "StringNotEquals": {  
11          "aws:sourceVpc": "vpc-06ebdcc366d35f277"  
12        }  
13      }  
14    },  
15    {  
16      "Effect": "Allow",  
17      "Principal": "*",  
18      "Action": "execute-api:Invoke",  
19      "Resource": "arn:aws:execute-api:us-east-2:373536100836:006bq9bckd/*"  
20    }  
21  ]  
22 }
```

API Gateway + VPC End Point


- POST 메소드로 키워드를 전송하면 결과를 반환
- API Gateway를 프라이빗으로 설정하여 외부에서 연결할 수 없도록 설정
- VPC 엔드 포인트 설정과 API 리소스 정책으로 내부 VPC에서 접근



AWS Architecture

웹 서비스 시연



 CVE SEARCHER

Sign UpSign In

Get Start to Search Vulnerability

검색



AWS Architecture

CVE SEARCHER

samba

검색

Sign Up

Sign In

KISA

[CVE-2018-17956](#)
7.8 CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
버전 1.0.1까지의 yast2-samba-provision에서 samba 공유에 대한 암호는 yast2-samba-provision에서 사용하는 도구에 대한 명령 줄에 제공되어 로컬 공격자가 프로세스 목록에서 읽을 수 있습니다.

[CVE-2020-25718](#)
8.8 CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Active Directory 도메인 컨트롤러인 삼바가 RODC(읽기 전용 도메인 컨트롤러)를 지원할 수 있는 방식에서 결함이 발견되었습니다. 이렇게 하면 RODC에서 관리자 티켓을 인쇄할 수 있습니다.

[CVE-2020-10704](#)

Exploit-DB

[Samba 2.2.x - Remote Buffer Overflow](#)
osvdb-4469 / cve-2003-0201 /

[Samba < 2.2.8 \(Linux/BSD\) - Remote Code Execution](#)
osvdb-4469 / cve-2003-0201 /

[Samba 2.2.8 - Brute Force Method Remote Command Execution](#)
osvdb-4469 / cve-2003-0201 /

[Microsoft Windows XP/2003 - Samba Share Resource Exhaustion \(Denial of Service\)](#)
osvdb-60587 /

CVE-Mitre

[CVE-2022-34298](#)
The NT auth module in OpenAM before 14.6.6 allows a "replace Samba username attack."

[CVE-2022-32746](#)
A flaw was found in the Samba AD LDAP server. The AD DC database audit logging module can access LDAP message values freed by a preceding database module, resulting in a use-after-free issue. This issue is only possible when modifying certain privileged attributes, such as userAccountControl.

[CVE-2022-32745](#)
A flaw was found in Samba. Samba AD users can cause the server to access uninitialized data with an LDAP add or modify the request, usually resulting in a segmentation fault.

Google

[Samba - opening windows to a wider world](#)
[www.samba.org](#)
Samba is the standard Windows interoperability suite of programs for Linux and Unix. Samba is Free Software licensed under the GNU General Public License, the ...Think Samba · Download · Samba Release History · Installing Samba

[Samba - Wikipedia](#)
[en.wikipedia.org](#) > wiki > Samba
Samba also known as samba urbano carioca (urban Carioca samba) or simply samba carioca (Carioca samba), is a Brazilian music genre that originated in the ...Brazilian dance · Samba (ballroom dance) · Samba (disambiguation) · Batucada



AWS Architecture

×

최근 검색 키워드

sam [삭제]

linux 3.2 [삭제]

samba [삭제]

samba

검색

HELLO [taejin]

log out

KISA

[CVE-2018-17956](#)

7.8 CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

버전 1.0.1까지의 yast2-samba-provision에서 samba 공유에 대한 암호는 yast2-samba-provision에서 사용하는 도구에 대한 명령 줄에 제공되어 로컬 공격자가 프로세스 목록에서 읽을 수 있습니다.

[CVE-2020-25718](#)

8.8 CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Active Directory 도메인 컨트롤러인 삼바가 RODC(읽기 전용 도메인 컨트롤러)를 지원할 수 있는 방식에서 결함이 발견되었습니다. 이렇게 하면 RODC에서 관리자 티켓을 인쇄할 수 있습니다.

Exploit-DB

[Samba 2.2.x - Remote Buffer Overflow](#)

osvdb-4469 / cve-2003-0201 /

[Samba < 2.2.8 \(Linux/BSD\) - Remote Code Execution](#)



VPC End Point의 보안 그룹 설정 미흡

인바운드 규칙 (2)							
<input type="text" value="보안 그룹 규칙 필터"/>							
<input type="checkbox"/>	Name ▼	보안 그룹 규칙 ID ▼	IP 버전 ▼	유형 ▼	프로토콜 ▼	포트 범위 ▼	소스
<input type="checkbox"/>	-	sgr-029938ab518d...	IPv4	HTTP	TCP	80	0.0.0.0/0
<input type="checkbox"/>	-	sgr-065be9b41ad7...	IPv4	HTTPS	TCP	443	0.0.0.0/0

- 프라이빗 API Gateway와 연결된 VPC 엔드 포인트의 **보안 그룹이 전체 IP로 허용**된 문제
- 퍼블릭 서브넷에서도 접근이 가능하기 때문에 프라이빗으로써의 기능이 무산된다.
- 프라이빗에 배치된 웹 서버에서만 이용하도록 하기 위해서 소스를 프라이빗 서브넷으로 수정하여 사용하는 것이 바람직하다고 생각된다.



보안 추가 보완점

네트워크 ACL 설정 미흡

네트워크 ACL (1/1) 정보

네트워크 ACL 필터링

Name	네트워크 ACL ID	연결 대상	기본값	VPC ID	인바운드 규칙
-	acl-07ba4cb5ce7bc6c0e	4 서브넷	예	vpc-06ebdcc366d35f277 / TAE-vpc	2 인바운드 규칙

acl-07ba4cb5ce7bc6c0e

세부 정보 | **인바운드 규칙** | 아웃바운드 규칙 | 서브넷 연결 | 태그

이제 Reachability Analyzer를 사용하여 네트워크 연결을 확인할 수 있습니다. Reachability Analyzer 실행

인바운드 규칙 (2)

인바운드 규칙 편집

인바운드 규칙 필터링

규칙 번호	유형	프로토콜	포트 범위	소스	허용/거부
100	모든 트래픽	모두	모두	0.0.0.0/0	Allow
*	모든 트래픽	모두	모두	0.0.0.0/0	Deny

- 디폴트 네트워크 ACL에 모든 서브넷이 적용되어있으며 인/아웃 바운드 규칙이 모두 허용된 문제
- 각각 서브넷의 기능에 따라 ACL을 적용하여 인/아웃 바운드 규칙을 설정한다면 더 세부적인 필터링이 가능할 것이라고 생각된다.



SQL injection 취약점 및 XSS 취약점 존재

로그인 페이지

`' or 1=1;--`

PW

로그인

HELLO [apink] log out

Get Start to Search Vulnerability

`<script>alert();</script>`

검색

52.14.219.21 내용:

1

확인

- 입력 데이터의 필터링이 제대로 설정되지 않아 SQLi 및 XSS 취약점이 존재하는 문제
- 입력되는 문자열은 적절한 필터링이나 `strip_tags`, `htmlspecialchars` 등의 시큐어 코딩 함수를 적용하여 문자열 이외의 기능을 하지 못하도록 제한한다.



로그인 데이터 평문 전송

```
1 POST /login.php HTTP/1.1
2 Host: 52.14.219.21
3 Content-Length: 22
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://52.14.219.21
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
  Gecko) Chrome/106.0.0.0 Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer: http://52.14.219.21/login.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
13 Cookie: PHPSESSID=ga9oce269q56054eltq5d0ldcm
14 Connection: close
15
16 logid=apink&logpw=love
```

- 데이터가 평문으로 전송되어 내용을 노출하는 취약점
- 전송 시 대칭키 암호화나 해시 혹은 HTTPS를 이용해 데이터를 암호화하여 전달해야 한다.



CSRF 취약점 존재

기존 서비스

52.14.219.21/register.php

회원 가입

회원 가입

카피 서비스

← → ↻ ⓘ 파일 | C:/Users/user/Desktop/csrf.html

회원 가입

```
mysql> select name,password from user_tbl;
+-----+-----+
| name  | password |
+-----+-----+
| taejin | 123      |
| tjmedia | score100 |
| majun  | 123123   |
| SooSeok | 1111     |
| apink  | love     |
+-----+-----+
5 rows in set (0.00 sec)
```

```
mysql> select name,password from user_tbl;
+-----+-----+
| name  | password |
+-----+-----+
| taejin | 123      |
| tjmedia | score100 |
| majun  | 123123   |
| SooSeok | 1111     |
| apink  | love     |
| hacker | hack     |
+-----+-----+
6 rows in set (0.00 sec)
```

- 웹 서비스 외부에서 웹 기능 요청이 정상 수행되는 문제
- 위 이미지는 로그인 폼을 추출한 html을 생성해서 hacker 계정을 생성한 모습이다.
- Referrer 검증, Security Token 사용하여 정상적인 행위로만 작동하도록 제한한다.



QnA