RC-LS, CheckEye DX - 機能改善 #4096

AWS_2023년12월5일 수신 내용

2023/12/05 12:42 - 金 英華

상태:	終了	**시작시간:**	2023/12/05
우선순위:	高め	**완료기한:**	2023/12/05
담당자:	朴 鎬秀	**진척도:**	0%
범주:		**추정시간:**	0.00 시간
목표버전:		**소요 시간:**	0.00 시간
システム:	CheckEye DX, RC-LS クラウド		

설명

AWS로부터 아래와같은 내용을 수신하였습니다.

확인 부탁드립니다.

Hello,

We've received a report(s) that your AWS resource(s)

AWS ID: 214387089372 Region: ap-northeast-1 EC2 Instance ID: i-06090ecf4c39cc52f
AWS ID: 214387089372 Region: ap-northeast-1 EC2 Instance ID: eni-0c8552565bbe749d6
AWS ID: 214387089372 Region: ap-northeast-1 EC2 Instance ID: i-04d829a04bd6e6ee7
AWS ID: 214387089372 Region: ap-northeast-1 EC2 Instance ID: eni-07fc674bcf115af97
AWS ID: 214387089372 Region: ap-northeast-1 EC2 Instance ID: i-06531f8c3abd7a0c6
AWS ID: 214387089372 Region: ap-northeast-1 EC2 Instance ID: eni-0f9e37a31c9ce004e
AWS ID: 214387089372 Region: ap-northeast-1 EC2 Instance ID: i-0bca6ddccf821330b
AWS ID: 214387089372 Region: ap-northeast-1 EC2 Instance ID: eni-038fa5b197a4db2ab
AWS ID: 214387089372 Region: ap-northeast-1 EC2 Instance ID: i-0de66d82c5afe2c20
AWS ID: 214387089372 Region: ap-northeast-1 EC2 Instance ID: eni-085310e6292b4ea0f

has been implicated in activity which resembles attempts to access remote hosts on the internet without authorization. Activity of this nature is forbidden in the AWS Acceptable Use Policy (https://aws.amazon.com/aup/). We've included the original report below for your review.

Please take action to stop the reported activity and reply directly to this email with details of the corrective actions you have taken. If you do not consider the activity described in these reports to be abusive, please reply to this email with details of your use case.

If you're unaware of this activity, it's possible that your environment has been compromised by an external attacker, or a vulnerability is allowing your machine to be used in a way that it was not intended.

We are unable to assist you with troubleshooting or technical inquiries. However, for guidance on securing your instance, we recommend reviewing the following resources:

* Amazon EC2 Security Groups User Guide:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html (Linux)
https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/using-network-security.html (Windows)

* Tips for Securing EC2 Instances:
https://aws.amazon.com/answers/security/aws-securing-ec2-instances (Linux)
https://aws.amazon.com/answers/security/aws-securing-windows-instances (Windows)

* AWS Security Best Practices:
https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf
https://aws.amazon.com/blogs/security/getting-started-follow-security-best-practices-as-you-configure-your-aws-resources/
https://docs.aws.amazon.com/security/?secd_intro2

If you require further assistance with this matter, you can take advantage of our developer forums:

https://forums.aws.amazon.com/index.jspa

Or, if you are subscribed to a Premium Support package, you may reach out for one-on-one assistance here:

https://console.aws.amazon.com/support/home#/case/create?issueType=technical

Please remember that you are responsible for ensuring that your instances and all applications are properly secured. If you require any further information to assist you in identifying or rectifying this issue, please let us know in a direct reply to this message.

Regards,
AWS Trust & Safety

Detailed abuse report information is included below.

```
=========================================================================
Resource: i-06090ecf4c39cc52f
Region: ap-northeast-1

Resource: eni-0c8552565bbe749d6
Region: ap-northeast-1

Abuse Case: 10684310798-1

-------------------------------------------------------------------------
Logs:
-------------------------------------------------------------------------
2023-11-10 11:58:01 GMT

{
"PORT HIT": "13.115.129.113:48780->103.#.#.10:23"
}

BitNinja automatically sets up honeypot ports on your server, running fake chatter services. The bad actor tried to connect to one of these services, and the connection was terminated.

=========================================================================
Resource: i-04d829a04bd6e6ee7
Region: ap-northeast-1

Resource: eni-07fc674bcf115af97
Region: ap-northeast-1

Abuse Case: 10684310798-2

-------------------------------------------------------------------------
Logs:
-------------------------------------------------------------------------
Time of catch: 2023-11-10 11:11:30 GMT

Incident content:

{
"PORT HIT": "3.115.113.235:39058->91.#.#.90:23"
}


BitNinja automatically sets up honeypot ports on your server, running fake chatter services. The bad actor tried to connect to one of these services, and the connection was terminated.

=========================================================================
Resource: i-06531f8c3abd7a0c6
Region: ap-northeast-1

Resource: eni-0f9e37a31c9ce004e
Region: ap-northeast-1

Abuse Case: 10684310798-3

-------------------------------------------------------------------------
Logs:
-------------------------------------------------------------------------
```

```
2023-11-10 11:25:07 GMT

{
"PORT HIT": "18.176.199.115:48640->194.#.#.56:23"
}

BitNinja automatically sets up honeypot ports on your server, running fake chatter services. The bad actor tried to connect to one of these services, and the connection was terminated.

========================================================================
Resource: i-0bca6ddccf821330b
Region: ap-northeast-1

Resource: eni-038fa5b197a4db2ab
Region: ap-northeast-1

Abuse Case: 10684310798-4

------------------------------------------------------------------------
Logs:
------------------------------------------------------------------------
2023-11-13 05:52:44 GMT

{
"PORT HIT": "13.112.21.8:39898->185.#.#.61:23"
}

BitNinja automatically sets up honeypot ports on your server, running fake chatter services. The bad actor tried to connect to one of these services, and the connection was terminated

========================================================================
Resource: i-0de66d82c5afe2c20
Region: ap-northeast-1

Resource: eni-085310e6292b4ea0f
Region: ap-northeast-1

Abuse Case: 10684310798-5

------------------------------------------------------------------------
Logs:
------------------------------------------------------------------------
2023-11-13 00:09:55 GMT

{
"PORT HIT": "54.199.48.12:58802->103.146.113.2:23"
}

BitNinja automatically sets up honeypot ports on your server, running fake chatter services. The bad actor tried to connect to one of these services, and the connection was terminated

========================================================================
Resource: i-0bca6ddccf821330b
Region: ap-northeast-1

Resource: eni-038fa5b197a4db2ab
Region: ap-northeast-1

Abuse Case: 10684310798-6

------------------------------------------------------------------------
Logs:
------------------------------------------------------------------------
Source IP / Targeted host / Issue processed @ / Log entry
---------------------------------------------------------------------------
* 13.112.21.8    tpc-024.mach3builders.nl    2023-11-12T16:19:34+01:00    16:19:25.644430 rule 0/0(match): block in on vmx0: 13.112.21.8.48586 > 91.190.98.122.23: Flags [S], seq 2257095372, win 0, options [mss 1460], length 0
* 13.112.21.8    tpc-test-001.mach3builders.nl    2023-11-06T22:22:54+01:00    23:22:52.605521 rule 0/0(match): block in on vmx0: 13.112.21.8.54228 > 91.190.98.12.23:
```

```
Flags [S], seq 292211436, win 0, options [mss 1460], length 0
* 13.112.21.8    tpc-019.mach3builders.nl    2023-11-04T21:21:23+01:00    22:21:13.560830 rule 0/0(match): block in on vmx0: 13.112.21.8.53490 > 91.190.98.195.23:
Flags [S], seq 828423345, win 0, options [mss 1460], length 0
* 13.112.21.8    tpc-019.mach3builders.nl    2023-11-04T21:21:22+01:00    22:21:13.497519 rule 0/0(match): block in on vmx0: 13.112.21.8.53528 > 91.190.98.195.23:
Flags [S], seq 901921602, win 0, options [mss 1460], length 0
* 13.112.21.8    tpc-041.mach3builders.nl    2023-11-03T17:38:34+01:00    18:38:30.744710 rule 0/0(match): block in on vmx0: 13.112.21.8.44124 > 91.190.98.14.23:
Flags [S], seq 1211534540, win 0, options [mss 1460], length 0
...


------------------------------------------------------------------------
Comments:
------------------------------------------------------------------------
========== X-ARF Style Summary ==========
Date: 2023-11-12T16:19:34+01:00
Source: 13.112.21.8
Type of Abuse: Portscan/Malware/Intrusion Attempts
```

연결된 일감:

다음 일감과 관련됨: RC-LS, CheckEye DX - リリース # 4082: [서버조치] EC2서...	**終了**	**2023/11/29**	**2023/11/29**

이력

#1 - 2023/12/05 13:16 - 朴 鎬秀

- 다음 일감과 관련됨:에 リリース #4082: [서버조치] EC2서버 메세지 브로커(ActiveMQ) 패치이(가) 추가되었습니다.

#2 - 2023/12/05 13:21 - 朴 鎬秀

- 설명이 변경되었습니다.
- 완료기한을(를) 2023/12/05(으)로 지정되었습니다.
- 상태을(를) 新規에서 進行中(으)로 변경되었습니다.

메세지 브로커(ActiveMQ) 의 취약점으로 인해 해당 EC2서버 공격을 받아 생긴 문제었습니다.

취약점 해결 버전 (#4082 참고) 으로 패치후 현재는 해당 문제 발생하지 않고 있습니다.

#3 - 2023/12/05 18:32 - 金 英華

- 상태을(를) 進行中에서 終了(으)로 변경되었습니다.

문제의 원인과 대응과정/결과에 관하여 AWS측에 답변 하였습니다.

추가 지시가 있으면 보고 드리겠습니다.