Twitter Thread by Scott Piper



Scott Piper
@0xdabbad00

As the year wrap's up, let's run through some of the worst public security mistakes and delays in fixes by AWS in 2020. A thread.

First, that time when an AWS employee posted confidential AWS customer information including including AWS access keys for those customer accounts to github.
https://t.co/3Y7vgOwDtV

> Fresh data breach news-
> Amazon AWS engineer exposes work-related keys, passwords, and documents marked "Amazon Confidential" via public Github repository: https://t.co/7gkIegnslx
> Discovered within 30 minutes of exposure by my team at @UpGuard.
>
> — Chris Vickery (@VickerySec) January 23, 2020

Discovery by @SpenGietz that you can disable CloudTrail without triggering GuardDuty by using cloudtrail:PutEventSelectors to filter all events. https://t.co/pR4TzI5xHV

> "Disable" most #AWS #CloudTrail logging without triggering #GuardDuty:https://t.co/zVe4uSHog9
>
> Reported to AWS Security and it is not a bug.
>
> — Rhino Security Labs (@RhinoSecurity) April 23, 2020

Amazon launched their bug bounty, but specifically excluded AWS, which has no bug bounty. https://t.co/bPSw6GbnoV

> Amazon Vulnerability Research Program - Doesn't include AWS D:https://t.co/stJHDG68pj#BugBounty #AWS
>
> — Spencer Gietzen (@SpenGietz) April 22, 2020

Repeated, over and over again examples of AWS having no change control over their Managed IAM policies, including the mistaken release of CheesepuffsServiceRolePolicy, AWSServiceRoleForThorInternalDevPolicy, AWSCodeArtifactReadOnlyAccess.json, AmazonCirrusGammaRoleForInstaller.

The worst IAM policy mistake came later in the year with ReadOnlyAccess purging all of its privileges to replace them with read/write access to cassandra. https://t.co/YI4Y32UPAR

> The ReadOnly IAM managed policy just had a huge purge of allowed actions.
>
> Some of the things it lost:
>
> * Billing
> * CodeArtifact
> * CodeBuild (some)
> * DeppComposer
> * FreeRTOS
> * Glue
> * Licence Manager
> * AWS SSO
>
> It gained access to sts:GetFederationToken and GetServiceBearerToken
>
> — Aidan W Steele (@__steele) October 16, 2020

Kesten shows a flaw in how many vendors use IAM roles. Although not technically a mistake by AWS (shared responsibility blah blah blah), this is something AWS is entirely capable of identifying and pushing vendors to correct, but did nothing. https://t.co/8KSZegSKqn

> We released my blog today: AWS IAM Assume Role Vulnerabilities Found in Many Top Vendors
> https://t.co/ug8hzx79QH
> I'll be presenting a lot more detail and variants on the attack at fwd:cloudsec https://t.co/6moTOQKFq1
>
> — kesten broughton BLM (@kestenb) June 17, 2020

AWS finally fixed a deficiency in the Route 53 and VPC APIs where if an attacker rerouted traffic via private hosted zones, you would not be able to audit for it. I list this here because this deficiency existed for 6 years! https://t.co/n3tnxEH1Lt

> Today is a good day for the security of AWS VPCs. A new API was released: route53:ListHostedZonesByVPC. This addresses a long-standing (six years!) deficiency in the Route 53 and VPC APIs.
>
> You can now list all private hosted zones associated with a given VPC. I'll try explain. pic.twitter.com/AVm2zsR43F
>
> — Aidan W Steele (@__steele) June 18, 2020

XSS on the web console. This issue was reported and fixed a few years ago but never disclosed until this year. https://t.co/6LksOQkXLw

> An older vulnerability write up about an XSS on the #AWS console which I responsibly disclosed to Amazon
>
> Hope its interesting for some who are getting started with #pentestinghttps://t.co/IGkS6LqiXw

> Also AMZN now awards #bugbounties via Hackerone. Check it out! No aws though
>
> — Johann Rehberger (@wunderwuzzi23) July 1, 2020

Discovery that in the terms and conditions of AWS, when using machine learning services, AWS will use your data to improve their services and move that data outside of the regions you put it in. This was added to the terms in late 2017 but not noticed. https://t.co/kZd8s4yCZc

> That has been hidden in the service terms. Interesting things to note:
> - data may leave the region
> - you can open a support case to opt out pic.twitter.com/so1QDeuXej
>
> — Ben Bridts\u200f (@benbridts) July 8, 2020

Crypto vulns found in AWS SDKs by Google employee @SchmiegSophie
https://t.co/D8w7mtR5yV

> After some final wrestling with CVSS, here my security advisory and proof of concept for three issues I've found in the golang AWS S3 crypto SDK (similar issues have been in the other language versions as well, but I didn't look at them).
>
> The issues are fixed for new files in V2 https://t.co/slUu9h5NWg
>
> — Dr. rer. nat. Sophie, her arms wide (@SchmiegSophie) August 10, 2020

AWS finally provides a fix for the HTTP desync issues that had been reported to them almost a year prior https://t.co/8tXOoFArw3 and https://t.co/9hXvh6dEZh

> Today, ELB has two cool releases that are worth a thread! The new DESYNC mitigation mode, https://t.co/MXv9PtmO6H, and open sourcing the HTTP Desync Guardian, https://t.co/yi8PDeg7vC, the anti-DESYNC rust library that we developed at AWS. 1/n
>
> — Colm MacC\xe1rthaigh (@colmmacc) August 17, 2020

AWS released CloudTrail Insights as a separate service, instead of integrating that functionality into GuardDuty. https://t.co/Z2TCcl9bpI ■■

> AWS CloudTrail now provides relevant user statistics to act on anomalies detected by CloudTrail Insights
>
> CloudTrail Insights now helps you correlate user identities, user agents, and error codes associated with unusual levels of API activity. Now, ... https://t.co/euHA4HgSuu
>
> — What\u2019s New on AWS (@awswhatsnew) August 25, 2020

AWS continues to make a mess of their managed IAM policies, creating AWS_Config_Role, AWS_ConfigRole, AWSConfigRole and AWSConfigServiceRolePolicy, along with 3 versions of AmazonMachineLearningRoleforRedshiftDataSource https://t.co/aK4c6ZVmYj https://t.co/Dao9JuXydU

> Wonder why we now have AWS_Config_Role, AWS_ConfigRole, AWSConfigRole and AWSConfigServiceRolePolicy that all appear to fill the same purpose? https://t.co/K7dQutisBE
>
> — Ben Reser (@BenReser) September 15, 2020

Aiden manages to gain access to an AWS account run by AWS for one of their services where he was then able to see credentials to gain access to AWS customer accounts. This is IMHO the most epic issue of the year for AWS. https://t.co/qucuKEzNd3

> Part 4 (of 5) of the series I wrote with @iann0036 is now up.
>
> This time it's a story about AWS CloudFormation potentially exposing credentials to customer AWS accounts - and how quickly the service team fixed it. https://t.co/BCLZxuaUlL
>
> — Aidan W Steele (@__steele) September 22, 2020

Karim does a security audit of an AWS project, that points out enough issues that AWS deprecates the project. https://t.co/jBLzEMJ5KX

> A security review of AWS CloudFormer (beta) reveals a bunch of vulnerabilities and some interesting findings https://t.co/E1dUwW8AIl #aws #cloudsecurity
>
> — Karim El-Melhaoui (@KarimMelhaoui) September 27, 2020

Another Google employee continues the trend of doing free work for AWS by finding more crypto issues: https://t.co/cjUV54g5ZE

> Someone told me that "Tink should follow AWS Encryption SDKs", so I showed them why Tink works the way it is and AWS SDKs were doing it wrong.
>
> Here are 3 vulnerabilities in AWS SDKs and AWS KMS. AMNZ has fixed them in release 2.0.0 of the SDKs:https://t.co/tamjxene1T
>
> — thaidn (@XorNinja) September 28, 2020

Ian finds tagging privileges are not properly enforced by AWS calling into question the ability to use ABAC as a security boundary. https://t.co/buuMhoQjL5

> For the final post in this series, we take a quick look at an issue that allowed for arbitrary tagging on #AWS S3 buckets and my (probably controversial) opinion on attribute-based access control. \u2601\ufe0f\U0001faa3\U0001f510https://t.co/yiIcMddJAn

> — Ian Mckay (@iann0036) September 29, 2020

Nick discovers a trick to test whether you have access to about 40 services without that testing being logged by CloudTrail. https://t.co/KJEjoiGuPm

> I recently found a bug in the AWS API that allows you to enumerate certain permissions for a role without logging to CloudTrail. It affects 645 actions in 40 AWS services. In this thread I'll provide a short tl;dr.https://t.co/YQrnf4Dg5z
>
> — Nick Frichette (@Frichette_n) October 17, 2020

AWS rolls out a new S3 web console which unfortunately once again allows people to set the "AuthenticatedUsers" ACL, which they haven't had in the console since 2017 because it is always misunderstood and wrong. https://t.co/VmKWySZtwE

> The new AWS S3 console is awesome! Much less of a chance to accidentally expose an S3 bucket. pic.twitter.com/pwlJhqNoPS
>
> — Spencer Gietzen (@SpenGietz) October 30, 2020

AWS released their SOC 2 Type 2 for April-Sep 2020, with concerning issues in it. Unfortunately you aren't allowed to discuss these reports, but the issues are on page 120 and 121.

That wraps things up. Let's hope AWS figures out wtf they are doing with IAM managed policies next year.

End.