AWS fixes security flaws that exposed AWS customer data

By
Sergiu Gatlan (https://www.bleepingcomputer.com/author/sergiu-gatlan/)

January 13, 2022 03:04 PM **0**

Amazon Web Services (AWS) has addressed an AWS Glue security issue that allowed attackers to access and alter data linked to other AWS customer accounts.

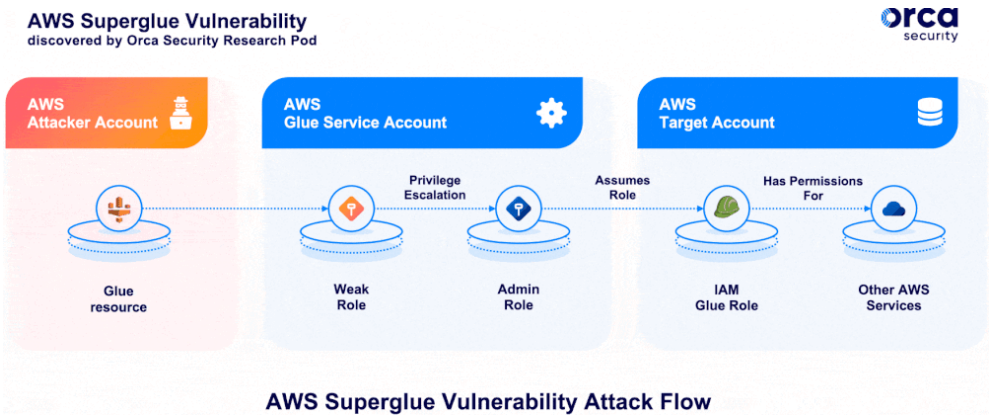
AWS Glue (https://aws.amazon.com/glue) is a serverless cloud data integration service that helps discover, prepare, and combine data for app development, machine learning, and analytics.

The flaw stemmed from an exploitable AWS Glue feature and an internal service API misconfiguration that allowed Orca Security security researchers to escalate privileges to gain access to all service resources in the region.

"During our research, we were able to identify a feature in AWS Glue that could be exploited to obtain credentials to a role within the AWS service's own account, which provided us full access to the internal service API," explained (https://orca.security/resources/blog/aws-glue-vulnerability/) Yanir Tsarimi, a Cloud Security Researcher at Orca Security.

"In combination with an internal misconfiguration in the Glue internal service API, we were able to further escalate privileges within the account to the point where we had unrestricted access to all resources for the service in the region, including full administrative privileges."

The researchers added that their findings were uncovered using only Orca Security-owned AWS accounts and that they didn't access information or data belonging to other AWS customers during their research.



AWS Superglue Vulnerability Attack Flow

While investigating the vulnerability, the researchers assumed roles trusted by the Glue service in other AWS customers' accounts (every account with Glue access has at least one such role).

They were also able to query and alter AWS Glue service-related resources in an AWS region, including but not limited to metadata for Glue jobs, dev endpoints, workflows, crawlers, and triggers.

The AWS Glue service team reproduced and confirmed the flaw within hours after receiving Orca Security's report and partially mitigated the issue globally by the following morning.

They deployed full mitigation for the Superglue vulnerability in just a few days, preventing potential attackers from accessing AWS Glue customers' data.

> *Analysis of logs going back to the launch of the service have been conducted and we have conclusively determined that the only activity associated with this issue was between accounts owned by the researcher. No other customer's accounts were impacted. All actions taken by AWS Glue in a customer's account are logged in CloudTrail records controlled and viewable by customers. — AWS (https://aws.amazon.com/security/security-bulletins/AWS-2022-002/)*

AWS' Security Team has also patched a second vulnerability (https://aws.amazon.com/security/security-bulletins/AWS-2021-007/) found by Orca Security in the AWS CloudFormation service (dubbed BreakingFormation (https://orca.security/resources/blog/aws-cloudformation-vulnerability/)).

According to the researchers, this XXE (XML External Entity) flaw led to file and credential disclosure of internal AWS infrastructure services.

"Our research team believes, given the data found on the host (including credentials and data involving internal endpoints), that an attacker could abuse this vulnerability to bypass tenant boundaries, giving them privileged access to any resource in AWS," Orca Security's Tzah Pahima added.

However, AWS VP Colm MacCárthaigh denied the security firm's claims, saying that the BreakingFormation bug could have only been used to access host-level credentials and that AWS CloudFormation hosts don't have access to resources in all AWS accounts.

Update January 13, 17:07 EST: An AWS spokesperson sent the following statement after the article was published:

> *We are aware of an issue related to AWS Glue ETL and AWS CloudFormation and can confirm that no AWS customer accounts or data were affected. Upon learning of this matter from Orca Security, we took immediate action to mitigate it within hours and have added additional controls to the services to prevent any recurrence.*

Related Articles:

27 flaws in USB-over-network SDK affect millions of cloud users (https://www.bleepingcomputer.com/news/security/27-flaws-in-usb-over-network-sdk-affect-millions-of-cloud-users/)

Android users can now disable 2G to block Stingray attacks (https://www.bleepingcomputer.com/news/security/android-users-can-now-disable-2g-to-block-stingray-attacks/)

Netgear leaves vulnerabilities unpatched in Nighthawk router (https://www.bleepingcomputer.com/news/security/netgear-leaves-vulnerabilities-unpatched-in-nighthawk-router/)

CISA alerts federal agencies of ancient bugs still being exploited (https://www.bleepingcomputer.com/news/security/cisa-alerts-federal-agencies-of-ancient-bugs-still-being-exploited/)

Microsoft January 2022 Patch Tuesday fixes 6 zero-days, 97 flaws (https://www.bleepingcomputer.com/news/microsoft/microsoft-january-2022-patch-tuesday-fixes-6-zero-days-97-flaws/)