ITC SECURE

Microsoft Solutions Partner

itcsecure.com

# ITC Secure

## Insurance Cloud Breaches

15 February 2023

# Cloud Breaches 2022 - lessons learnt and outlook for 2023

The cloud is becoming more prevalent in the insurance industry as more companies make the transition to the digital world and rely on the experience of cloud providers to share data quickly across platforms to drive greater efficiencies.

Migrating data and platforms to the cloud can offer many benefits such as elasticity, availability and redundancy, providing a more dynamic and cost-effective alternative to support businesses growth aspirations.

Although there are many benefits to the cloud, it has recently emerged as a growing attack vector for many of the major security breaches in 2022.

In this report, ITC Secure looks back at some of the cloud data breaches that were publicly disclosed in 2022, focusing on breaches from organisations using major cloud providers such as AWS, Azure and Google Cloud.

This report will look at the major patterns of security breaches in 2022, what insecure configurations attackers have been able to exploit, as well as highlight what lessons can be learnt from these incidents and how this can help carriers, brokers, and reinsurers in 2023.

Before we dive in, we want to emphasise that this is a blame-free article. Securing cloud environments is a challenge for everyone, and companies that publicly report their incidents should not be criticised for choosing to be transparent.

## 1) Exposed, long-lived cloud credentials

In cloud environments, open Application Programming Interfaces (APIs) are, by design, available for anyone on the internet to use. As a result, compromising long-lived credentials has been the most popular way for attackers to gain access to cloud environments for years.

In 2022, it was confirmed that many long-lived cloud credentials were exposed, and GitHub repositories compromised, including AWS, Google Cloud and Microsoft.  In some cases, access keys and private repositories were accidentally published. Overall, many people store important keys and credentials in GitHub and the tools that attackers can use to detect and steal those keys are becoming more accessible and efficient.

We also see a continuing trend where credentials are included in public software packages such as Android applications and PyPI (Python Package Index) packages, making them easy for attackers to discover.

Finally, attackers continue to target developers in the software supply chain. In particular, several malicious PyPI and npm (Node Package Manager) packages have actively attempted to steal cloud credentials.

## 2) Vulnerable Elasticsearch instances

Not surprisingly, technologies that are insecure by default without the cloud are also configured insecurely in the cloud. This is the case with Elasticsearch, Redis or MongoDB, which do not enforce authentication by default.

In 2022, at least three data breaches were reported related to insecurely configured Elasticsearch instances in AWS. It is not clear whether these were customer managed Elasticsearch instances running on EC2 or misconfigured clusters using the managed OpenSearch service. Interestingly, one of these misconfigurations came from a division of Amazon itself.

An example of configuration that isn't enabled by default is the Elasticsearch version 1.3.7 shipped with the "groovy scripting engine" enabled by default. Vulnerabilities within the scripting engine allow attackers to construct scripts that escape the sandbox and execute shell commands as the user running the Elasticsearch Java VM.

Simply setting "script.groovy.sandbox.enabled" to "false" resolves the CVSS rated 7.5 vulnerability.

## 3) Storage services with public access

Public Amazon S3 (Amazon Simple Storage Service) buckets have been a common cause of data breaches for nearly a decade, and again in 2022 there were nearly 20 publicly reported data breaches. We have also seen several cases of security breaches due to public Azure Blob Storage, including from Microsoft itself. Attackers can easily scan for and compromise dangerously configured storage buckets due to the variety of tools available and the increasing number of bug bounties.

Researchers also identified hundreds of unprotected Amazon RDS snapshots, some of which contained a wealth of sensitive and personal data.

AWS added public sharing of snapshots in 2015, responding to requests from the data science community. AWS introduced open data that same year, but one community's feature request is another community's new risk: a seemingly inevitable part of progress.

## 4) Server-side request forgery (SSRF) security vulnerabilities

Cloud virtual machines such as AWS EC2 instances or Google Cloud Compute Engine instances are often assigned a role that allows the applications they run to access the cloud provider's API. However, if the instance is not hardened, an attacker exploiting an SSRF vulnerability can also retrieve the cloud credentials for the assigned instance role.

Exploitation of SSRF vulnerabilities in cloud environments has been a major problem for years. Earlier this year, we found that 93 percent of EC2 instances still allow the use of Instance Metadata Service v1, putting them at risk if an application vulnerable to SSRF is running.

This continues to be a significant risk and is the reason for numerous vulnerability and bug bounty reports in 2022, especially considering that SSRF vulnerabilities are prevalent in applications with over 380 CVEs reported in 2021.

## Some of the lessons learnt from the cloud breaches of 2022

The problem of sensitive data being leaked from public storage buckets is not new. In fact, tools to identify vulnerable buckets have been around since 2011.

The companies leaking S3 buckets are different from those of 2015; we see many small businesses and non-core divisions of large companies, but fewer startups whose entire business runs through an open S3 bucket. These types of data breaches will always exist. It's easier these days to discover open buckets and monetise them through bug bounties or ransomware.

Long-lived, static cloud credentials are still one of the most common causes of data breaches in the cloud. While there are better alternatives for both applications and people, this is only part of the problem. As we see with SSRF exploitation, the elephant in the room is credential portability. When retrieving temporary credentials for an EC2 profile from a particular instance, one should only be able to use them from that aligned instance.

While cloud providers now offer protections such as AWS's account-wide S3 Block Public Access or Azure Blob Storage's similar account-wide feature, many organisations do not have enough staff to understand these protections, especially if they are not enabled by default.

Cloud providers need to make it increasingly difficult to make critical mistakes. Microsoft has introduced several mechanisms to enable a secure default setting, including encryption, support for custom guardrails with service control policies, and console enhancements.

A proactive approach by providers can be complementary. For example, a few years ago AWS started emailing customers that had risky configurations such as public S3 buckets, public AMIs, public EBS snapshots or internet-exposed reverse proxies that allowed access to the instance metadata service. The more complex a system is, the more likely it is to be abused and a security breach will occur. No one is immune to misconfiguration, not even the cloud providers themselves. Since cloud providers tend to be large companies that have numerous business units with very different focuses, they too are at risk of making mistakes when engineers misconfigure their own public cloud services.

While this is not necessarily new, cloud providers now have more visibility when there is a breach caused by incorrect use of the services they sell - partly because there are more organisations working to detect and monetise them. Cloud providers also need to strike a balance between disclosing data and protecting the privacy of their customers. Currently, there is no simple solution for reporting and anonymising these incidents. We hope that this will be possible in the future.

Until then, there is still a long way to go ...

## Conclusion

The incidents discussed in this report are only those that have been made public. While organisations that make their incidents public are a great education asset to our community, most incidents still go unreported because of the tangible costs and risks involved.

While it is unlikely that most organisations will start reporting their security incidents out of pure altruism, cloud providers themselves have a role to play.

Indeed, providers are slowly starting to publish all the customer incidents they are aware of. At Re:Inforce 2022, AWS showcased common tactics used by attackers targeting S3 buckets with ransomware. The recent creation of the AWS Customer Incident Response Team is an initiative that will hopefully provide more visibility into the threats that enterprises face in cloud environments. Google's Cybersecurity Action Team also regularly publishes "Threat Horizon" reports describing the most common attacker tactics they observe in the Google Cloud. However, there is still room for improvement.

Remember the importance of:

- Detecting and mitigating legacy vulnerabilities before migrating to the cloud.
- Removing reliance on long-lived credentials and consider a cloud-based identity solution which suits your organisation’s needs.
- Regularly revisit your cloud strategy and controls with third-party specialists who can audit your environment independently and neutrally.

Jalil Neghza, senior executive and industry officer for the insurance sector at ITC Secure, highlights that today, many professionals responsible for cyber security still often dread the reputational damage associated with a security breach. This is a complex problem that is indeed a double-edged sword, as sharing information about security breaches could be used by hackers to target new victims. Equally, refusal to share information about a breach has resulted in large fines for insurance companies

## About ITC Secure

As a specialised Microsoft Solutions Partner in Security, ITC Secure has invested in building capabilities in Cloud Security, Identity and Access Management and Threat Protection. With an in-depth understanding of emerging technologies and the threat landscape we can quickly map business requirements to deliver tangible impact.

For a closer look at common cloud misconfigurations in the real world and how to fix them, do not hesitate to get in touch. One of our cloud experts can help your teams assess your current cloud infrastructure, identify potential vulnerabilities and recommend corrective actions to reduce your attack surface. Moreover, we can provide advice on the latest trends in securing the cloud and help you achieve your business goals in 2023.

*The data in this paper was gathered from a wide range of publicly available sources (details of which can be provided upon request).*