Cloud | 3 MIN READ NEWS

Attackers Can Compromise Most Cloud Data in Just 3 Steps

An analysis of cloud services finds that known vulnerabilities typically open the door for attackers, while insecure cloud architectures allow them to gain access to the crown jewels.

Robert Lemos
Contributing Writer, Dark Reading

September 13, 2022

Source: Mark Andrew Thomas via Alamy Stock Photo

Companies and their cloud providers often leave vulnerabilities open in their system and services, gifting attackers with an easy path to gain access to critical data.

According to an Orca Security analysis of data collected form major cloud services and released on Sept. 13, attackers only need, on average, three steps to gain access to sensitive data, the so-called "crown jewels," starting most often — in 78% of cases — with the exploitation of a known vulnerability.

While much of the security discussion has focused on the misconfigurations of cloud resources by companies, cloud providers have often been slow to plug vulnerabilities, says Avi Shua, CEO and co-founder of Orca Security.

"The key is to fix the root causes, which is the initial vector, and to increase the number of steps that they attacker needs to take," he says. "Proper security controls can make sure that even if there is an initial attack vector, you are still not able to reach the crown jewels."

The report analyzed data from Orca's security research team using data from a "billions of cloud assets on AWS, Azure, and Google Cloud," which the company's customers regularly scan. The data included cloud workload and configuration data, environment data, and information on assets collected in the first half of 2022.

Unpatched Vulnerabilities Cause Most Clou isk

"There is room for improvement on both sides of the shared responsibility model," Shua says. "Critics have always focused on the customer side of the house (for patching), but in the past few years, there have been quite a few issues on the cloud-provider end that have not been fixed in a timely manner."

In fact, fixing vulnerabilities may be the most critical problem, because the average container, image, and virtual machine had at least 50 known vulnerabilities. About three-quarters — 78% — of attacks start with the exploitation of a known vulnerability, Orca stated in the report. Moreover, a tenth of all companies have a cloud asset using software with a vulnerability at least 10 years old.

Yet the security debt caused by vulnerabilities is not evenly distributed across all assets, the report found. More than two-thirds — 68% — of Log4j vulnerabilities were found in virtual machines. However, only 5% of workload assets still have at least one of the Log4j vulnerabilities, and only 10.5% of those could be targeted from the Internet.

Customer-Side Issues

Another major problem is that a third of companies have a root account with a cloud provider that is not protected by multifactor authentication (MFA). Fifty-eight percent of companies have disabled MFA for at least one privileged user account, according to Orca's data. Failing to provide the additional security of MFA leaves systems and services open to brute-force attacks and password spraying.

In addition to the 33% of firms lacking MFA protections for root accounts, 12% of companies have an Internet-accessible workload with at least one weak or leaked password, Orca stated in its report.

Companies should look to enforce MFA across their organization (especially for privileged accounts), assess and fix vulnerabilities faster, and find ways to slow down attackers, Shua says.

"The key is to fix the root causes, which is the initial vector, and to increase the number of steps that the attacker needs to take, " he says. "Proper security controls can make sure that even if the attacker has success with the initial attack vector, they are still not able to reach the crown jewels."

Overall, both cloud providers and their business clients have security issues that need to be identified and patched, and both need to find ways to more efficiently close those issues, he adds; visibility and consistent security controls across all aspects of cloud infrastructure is key.

"It is not that their walls are not high enough," Shua says. "It is that they are not covering the entire castle."

Threat Intelligence Attacks/Breaches Application Security