Leaky Buckets: 10 Worst Amazon S3 Breaches

By Ericka Chickowski on Jan 24, 2018 | 0 Comments

The last year has proved out about security naysayers' warnings about the undisciplined use of cloud architectures. While many organizations work hard to secure data stored on cloud stores, the truth is that there's a lot of work to go. That fact is made abundantly clear by the growing number of incidents caused by extremely poor security hygiene within Amazon Simple Storage Service (S3) storage buckets that are holding very sensitive information.

According to recent statistics, as many as 7% of all S3 servers are completely publicly accessible without any authentication and 35% are unencrypted. And if the incidents of the past six months or so are any indication, these aren't low-value data stores. Here are some of the worst recent leaks caused by poorly configured Amazon S3 resources.

Keybase

{keybase} • https://github.com/ropenscilabs/keybase