NETSPI FIELD NOTES

# Application Server Returns Privileged User Keys to Unauthenticated Users

**Cloud & Mobile Application Penetration Testing**

## Situation

NetSPI consultants were testing a mobile application (iOS & Android) on behalf of a global data and analysis company. The mobile application was using a cloud service provider (AWS) to host backend services.

## Process

The test began by proxying network traffic between the mobile application and the backend server. The testers used Burp Suite, an intercepting proxy. While viewing HTTP requests, NetSPI consultants noticed that the application server disclosed sensitive information in HTTP responses.

Upon further inspection, one of NetSPI's cloud security experts identified that a specific unauthenticated HTTP request prompted the application server to return a privileged AWS user's programmatic access keys. The team discovered that the AWS user associated with these keys had the ability to upload and download arbitrary files into sensitive s3 buckets.

Once the NetSPI team discovered that the server was leaking AWS user access keys, NetSPI immediately contacted the application team. As this vulnerability was discovered in a production environment, the testers understood the sensitivity surrounding this issue.

## Impact

Leveraging the AWS user keys, an unauthenticated attacker can upload and download sensitive or malicious files in s3 buckets.

## Recommendations

This vulnerability is a result of the application server sharing AWS user keys with unauthenticated users. To remediate, NetSPI advises against providing AWS user keys directly to the mobile application as a method for uploading or downloading files from s3 buckets. Rather, have the application server handle the uploading of files to s3 buckets. Then, have the server generate signed URLs to access files within s3 buckets. In doing so, application users will no longer have access to s3 user keys.

As more organizations adopt cloud infrastructure, utilizing cloud services securely is paramount. Although AWS and other cloud providers are robust, there is still a risk for misconfiguration and settings aren't always reliable. Moving applications to the cloud unfortunately doesn't make them secure by default. The paradigm is changing and NetSPI can help meet these evolving security needs.

**Learn More About NetSPI's Penetration Testing Services**

**Cloud Pentesting**
www.netspi.com/security-testing/cloud-penetration-testing

**Application Pentesting**
www.netspi.com/security-testing/application-penetration-testing