

TechAndComputer (June 20, 2011) □ Scientists from the Darmstadt Research Center for Advanced Security (CASED) have discovered major security vulnerabilities in numerous virtual machines published by customers of Amazon's cloud. Among 1100 public Amazon Machine Images (AMIs), which are used to provide cloud services, about 30 percent are vulnerable, allowing attackers to manipulate or compromise web services or virtual infrastructures, the researchers say.

The main reason lies in the careless and error-prone manner in which Amazon's customers handle and deploy AMIs. CASED scientists have developed a vulnerability scanner for virtual machines that customers create to run on Amazon's infrastructure. It can be freely downloaded at <http://trust.cased.de/AMID> .

Cloud computing is becoming increasingly popular. More and more companies and private users are offering services in the cloud. While security experts have been mainly focusing on security aspects of the underlying cloud infrastructure and provider, it seems that in practice the threats caused by the cloud customers when constructing services are still underestimated or ignored. How severe the consequences resulting from wrong user behaviour can be, has now been shown by recent analysis carried out by the research group led by Prof. Ahmad-Reza Sadeghi at CASED.

The scientists at Fraunhofer SIT in Darmstadt and the System Security Lab at the Technische Universität Darmstadt examined services published by customers of Amazon Web Services (AWS). Even though AWS provide their customers with very detailed security recommendations on their web pages, the scientists found that at least one third of the machines under consideration have flawed configurations. The research team could extract security critical data such as passwords, cryptographic keys and certificates from the analyzed virtual machines. Attackers can use such information to operate criminal virtual infrastructures, manipulate web services or circumvent security mechanisms such as Secure Shell (SSH).

"The problem clearly lies in the customers' unawareness and not in Amazon Web Services. We believe that customers of other cloud providers endanger themselves and other cloud users similarly by ignoring or underestimating security recommendations," emphasizes Prof. Sadeghi. In coordination with the Amazon Web Services' security team the affected customers have been informed.

Careless behaviour of cloud users leads to crucial security threats, experts find

Written by Editor
Monday, 20 June 2011 09:52

Email or share this story:

Story Source:

The above story is reprinted (with editorial adaptations by TechandComputer.com staff) from materials provided by

[Technische Universität Darmstadt](#)

, via

[AlphaGalileo](#)

Note: If no author is given, the source is cited instead.

Disclaimer: Views expressed in this article do not necessarily reflect those of TechAndComputer or its staff.