

Hacker Puts Hosting Service Code Spaces Out of Business

By Michael Mimoso

Published: 2014-06-18 · Archived: 2026-04-06 01:59:38 UTC

Cloud-based code-hosting service Code Spaces announced today it was going out of business after a hacker deleted most of its machines, customer data and backups.

Code Spaces, a code-hosting and software collaboration platform, has been put out of business by an attacker who deleted the company's data and backups.

Officials wrote a lengthy [explanation and apology](#) on the company's website, promising to spend its current resources helping customers recover whatever data may be left.

"Code Spaces will not be able to operate beyond this point, the cost of resolving this issue to date and the expected cost of refunding customers who have been left without the service they paid for will put Code Spaces in an irreversible position both financially and in terms of ongoing credibility," read the note. "As such at this point in time we have no alternative but to cease trading and concentrate on supporting our affected customers in exporting any remaining data they have left with us."

The beginning of the end was a DDoS attack initiated yesterday that was accompanied by an intrusion into Code Spaces' Amazon EC2 control panel. Extortion demands were left for Code Spaces officials, along with a Hotmail address they were supposed to use to contact the attackers.

"Upon realization that somebody had access to our control panel, we started to investigate how access had been gained and what access that person had to the data in our systems," Code Spaces said. "It became clear that so far no machine access had been achieved due to the intruder not having our private keys."

Code Spaces said it changed its EC2 passwords, but quickly discovered the attacker had created backup logins, and once recovery attempts were noticed, the attacker began deleting artifacts from the panel.

"We finally managed to get our panel access back, but not before he had removed all EBS snapshots, S3 buckets, all AMI's, some EBS instances and several machine instances," Code Spaces said. "In summary, most of our data, backups, machine configurations and offsite backups were either partially or completely deleted."

"In summary, most of our data, backups, machine configurations and offsite backups were either partially or completely deleted."

[Amazon Web Services](#) customers are responsible for credential management. Amazon, however, has built-in support for two-factor authentication that can be used with AWS accounts and accounts managed by the AWS Identity and Access Management tool. AWS IAM enables control over user access, including individual credentials, role separation and least privilege.

Within 12 hours, Code Spaces went from a viable business to devastation. The company reported that all of its svn repositories—backups and snapshots—were deleted. All EBS volumes containing database files were also deleted. A few old svn nodes and one git node were left untouched, the company said.

A [cache](#) of Code Spaces services includes promises of full redundancy and that code is duplicated and distributed among data centers on three continents.

“Backing up data is one thing, but it is meaningless without a recovery plan, not only that a recovery plan – and one that is well-practiced and proven to work time and time again,” Code Spaces said. “Code Spaces has a full recovery plan that has been proven to work and is, in fact, practiced.”

Source: <https://threatpost.com/hacker-puts-hosting-service-code-spaces-out-of-business/106761/>