A Misconfigured Amazon S3 Exposed Almost 50 Thousand PII in Australia

Archived: 2026-04-05 14:53:34 UTC

A misconfigured Amazon S3 bucket has accidentally compromised 48,270 personally identifiable information (PII) from Australian employees working in government agencies, banks, and a utility company. The leaked PIIs include full names, passwords, IDs, phone numbers, email addresses, and some credit card numbers. Salary and expense details were also exposed.

25,000 staff records involving internal expenses from insurance company AMP were exposed, while utility company UGL had 17,000 records exposed. Affected government agencies include the Australian Department of Finance (3,000 employee records breached) and the Australian Electoral Commission (1,470), while the National Disability Insurance Agency had their details openly accessible. 1,500 employees at Rabobank were also affected.

The Department of Prime Minister and Cabinet stated that when the Australian Cyber Security Centre (ACSC) became aware of the situation, they immediately contacted the external contractor and worked with them to secure the information and remove the vulnerability.

"Now that the information has been secured, the ACSC and affected government agencies have been working with the external contractor to put in place effective response and support arrangements," they added.

Amazon S3 is a highly scalable cloud storage service where employees can store and retrieve data from websites and mobile apps. The PIIs were reportedly exposed following a misconfiguration on the system's Amazon S3 bucket. No foul play has been suspected so far; the cause of the accidental breach points to an unnamed third-party contractor not properly securing the web service.

This data breach incident is not the first one involving misconfigured Amazon S3 buckets this year. Financial publishing firm Dow Jones & Company exposed data including names, addresses, and partial credit card numbers of 2.2 million customers. Researchers also discovered a trove of sensitive corporate data in a publicly accessible Amazon S3 bucket owned by Verizon. Thousands of files containing PII of US citizens with classified security clearance were also compromised.

This latest incident follows the massive data breach that took place in Australia a year ago when 1.2 million records relating to 550,000 blood donor applicants from the Australian Red Cross Blood Service were exposed. The private information contained in the leaked records included answers to a sensitive question on whether the applicant had engaged in risky sexual behavior over the past year. Other compromised information included names, blood types, birth dates, email and snail mail addresses and phone numbers.

Solutions

Trend Micro Deep Security as a Service is optimized for AWS, Azure, and VMware to protect servers instantly. It reduces strain on your overburdened IT department by offloading security set up, management, and system updates to Trend Micro. Deep Security as a Service can start securing servers immediately without system installation or configuration.

Organizations should also choose the right cloud security solution for their organizations based on what can give them the most protection. Trend Micro Deep Security for Cloud can provide proactive detection and prevention of threats, while Hybrid Cloud Security provides optimal security for hybrid environments that incorporate physical, virtual, and cloud workloads.

HIDE

Like it? Add this infographic to your site:

1. Click on the box below. 2. Press Ctrl+A to select all. 3. Press Ctrl+C to copy. 4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.
