COVID tests may leak personal data

February 15 2022, by Petra Wester

Alexandre Bartel, Professor at the Department of Computing Science, have discovered a discovered a critical security weakness in the handling of COVID tests. Credit: Mattias Pettersson

Last year, over 14 million PCR tests were performed in Sweden. Researchers at Umeå University have discovered that personal data has been exposed by a private company handling test certificates. "This is something that may have affected thousands of Swedes," says Alexandre Bartel, WASP professor and head of the Software Engineering and

Security research group at the Department of Computer Science, Umeå University.

In Sweden, when you take a PCR test to have a certificate issued, your personal data are handled by private companies. Alexandre Bartel and his research group have discovered a critical security weakness at such a company that handles these certificates in all major cities in Sweden.

"We were able to access personal information, ranging from names and social security numbers to where the test was performed and what the results were by forcing the server to run in an unexpected state," says Alexandre Bartel.

Since these private companies do not communicate on the number of tests they handle, it is still unclear how many persons could be affected by such a vulnerability.

"Nevertheless, we have been informed that it could have had impacted at least thousands of people" says Alexandre Bartel.

The problem is solved, for now

When Alexandre discovered the problem in July 2021, he immediately contacted the company. With his help, the company—which does not want to be named—was able to quickly find and fix the weakness within 24 hours. At the same time, the company was able to ensure that no one else had discovered and exploited this vulnerability.

"The company claims that it was able to verify that no leakage of data or personal information had occurred. They were very grateful, and at the same time they have now realized that although they know that a high level of security is essential to handle this kind of information, a thorough evaluation of the security of the entire software system is a

must," says Alexandre Bartel. The company also says it welcomes future collaboration with Umeå University on this topic.

Health related data still at risk?

For most people, it goes without saying that personal data, especially data related to health, is handled securely. In practice, data can be shared and/or stored between multiple institutions or companies which might increase the attack surface. From the point of view of an attacker finding one vulnerability in the weakest link allows to expose the data.

"One reason why data leakage problems can occur is because companies handling the data only have to comply with Swedish laws and meet a list of requirements," says Alexandre Bartel.

Unfortunately, being compliant to a list of requirements does not mean that a system is secure. Furthermore, no auditing of the real running system including its software stack is mandatory yet. Thus, configuration or implementation weaknesses can pass under the radar.

"All companies develop their own systems or purchase a license for one. This means that similar problems can be found in several other companies," continues Alexandre.

Security at an early stage

There are two main aspects to security problems. The first is data leakage, where an external party can see and gain access to personal data and the like. The second is when an external actor can get into a system and manipulate the data. By building the system with security in mind from the outset and allowing a third party to evaluate the system, leakage and other attacks can be minimized, which is particularly important when personal data is involved.

"Sadly, most people think about security far too late. It is seen primarily as a cost, and the benefits of high security are often invisible. To prevent problems, the system should be designed from a security perspective at an early stage and evaluated by a third party," says Alexandre Bartel.

Companies are encouraged to follow this process because if they are affected by a leak of personal data, they would be in violation of GDPR and could get fined up to 4% of their annual revenue.

Automated tool

Alexandre Bartel and his research team at the Department of Computer Science are working, among other things, on developing software tools that can detect weaknesses automatically, thus minimizing data leakage and the risk of attacks. One of the goals is to reduce the time and computational resources required.

"We are working to develop solutions that can efficiently find weaknesses in systems, making it easier to prevent them and manage them," says Alexandre Bartel.

Provided by Umea University

Citation: COVID tests may leak personal data (2022, February 15) retrieved 27 March 2023 from https://techxplore.com/news/2022-02-covid-leak-personal.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.