Singtel, QIMR Berghofer report Accellion-related data breaches

By Lawrence Abrams

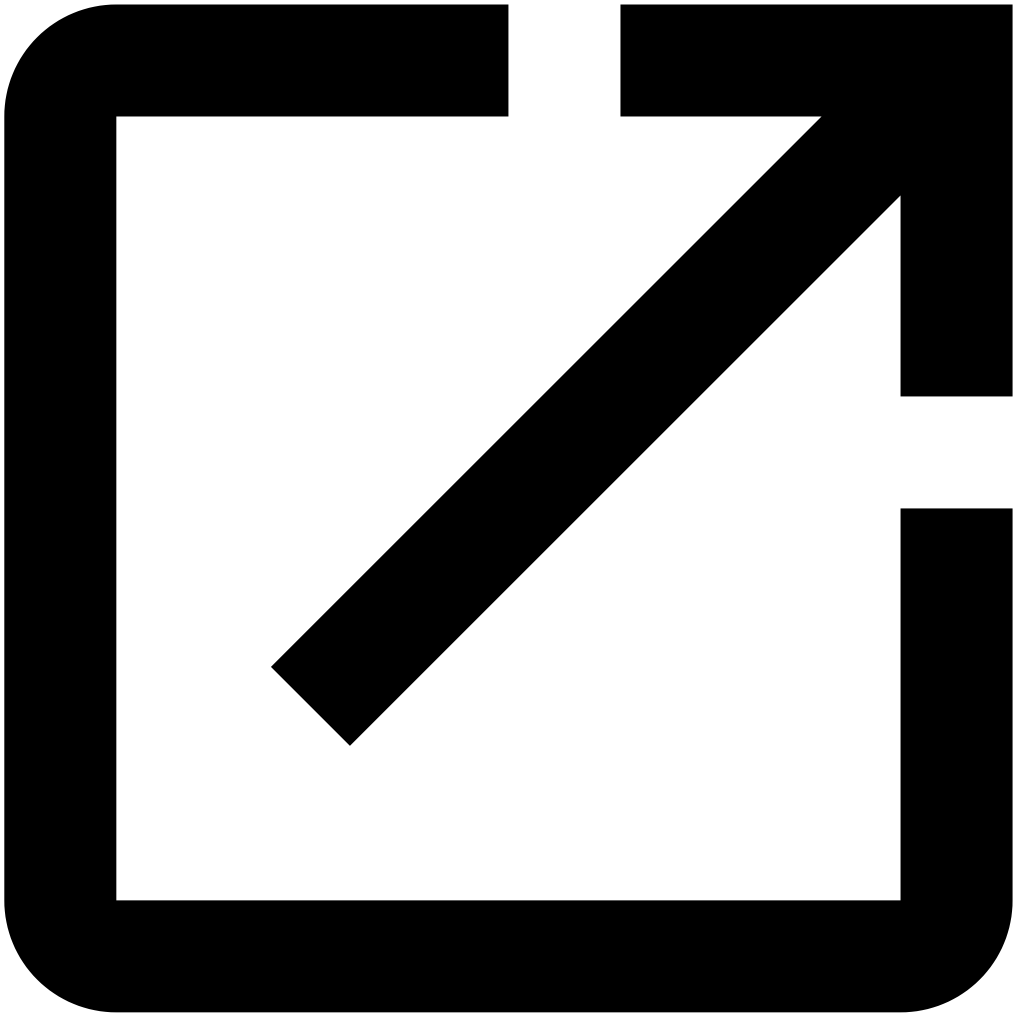
Published: 2021-02-11 · Archived: 2026-04-05 15:13:05 UTC

Singtel and the QIMR Berghofer Medical Research Institute are the latest companies to disclose data breaches caused by a vulnerability in the Accellion FTA secure file transfer software.

Accellion is a developer of secure file transfer products that allow organizations to transfer sensitive files with people outside of their organization.

In mid-December, Accellion announced that they became aware of an actively exploited zero-day vulnerability in their FTA secure file transfer product that allowed threat actors to access customers' data.


DIE LINKE.
0:00



While they released a patch on Christmas day as soon as they learned of the vulnerability, by the time some companies were able to patch, threat actors had already gained access to their data.

As Accellion FTA service is used by numerous government agencies, educational institutions, and companies, we have begun to see a wide-scale impact as companies report related data breaches.

Previous data breaches include the Reserve Bank of New Zealand, the Australian Securities and Investments Commission (ASIC), and the Office of the Washington State Auditor ("SAO").

The Singtel data breach

Singtel, the largest mobile carrier in Singapore, announced today that they suffered a data breach caused by the Accellion FTA service's vulnerability.

"A third-party file sharing system provided by Accellion called FTA has been illegally accessed through a zero-day vulnerability or previously unknown vulnerability. Singtel uses this system to share information internally as well as with external stakeholders and organisations," Singtel announced in a security incident notification.

The telecommunications company has not disclosed what data has been accessed in the attack and states that they are currently investigating who was impacted.

"Given the complexity of the investigations, it will take time to make an impact assessment. We are working with the utmost urgency to ascertain the nature and extent of data that has been potentially accessed. We will reach out to individuals and organisations whose information may have been illegally downloaded," Singtel continued.

While investigations are underway, Singtel states that they have taken the FTA system offline while they perform an investigation into the breach.

Once it is determined what the threat actors accessed, they will begin contacting affected people.

QIMR Berghofer affected as well

The QIMR Berghofer Medical Research Institute has also announced today a data breach caused by the Accellion FTA service and has provided more detailed information regarding what information was accessed.

According to the research institute, the data breach appears to have occurred on December 25, 2020, when threat actors accessed approximately 4 percent, or 620MB, of data stored on the Accellion FTA service.

QIMR Berghofer states that they received their first notification to install Accellion's patch on January 4th, 2021. It wasn't until February 2nd, 2021 that Accellion notified them that they had suffered a data breach.

"The first notification QIMR Berghofer received from Accellion was on 4 January 2021, when the company advised the Institute to apply a security patch. The Institute immediately took the software offline and applied the patch."

"Accellion notified QIMR Berghofer on Tuesday 2 February 2021 that it believed the Institute had been affected by the data breach, which has also affected a number of Accellion’s other Australian and international clients," QIMR Berghofer disclosed in a data breach notice on their website.

The research institute states that they utilize the FTA service to receive and send data regarding clinical trials for anti-malaria drugs, and to share data with the Mosquito and Arbovirus Research Committee.

However, the shared data is anonymized before being stored on Accellion, and trial participants are assigned codes to identify them.

The "de-identified" information stored by them on Accellion includes initials, date of birth, age, gender, and ethnic group of clinical trial participants, as well as the participant codes. Some documents also have a de-identified medical history.

QIMR Berghofer also states that the resumes for approximately 30 employees on the Accellion FTA service.

The lack of identifying information in the data stored on the FTA device is a double-edged sword.

While no personally identifying information has been disclosed, as each trial participant has been de-identified and assigned codes to refer to them, QIMR Berghofer has no way to contact them.

“We cannot contact these clinical trial participants because we don’t know who they are, and don’t have their names or contact details. However, if anyone has any concerns, or would like more information, they can contact us via the details below.

“We are contacting our clinical trial partners and other stakeholders to let them know what has happened and what we are doing to address this likely data breach," explains QIMR Berghofer.

Thanks to Douglas Mun for the tip.

Source: https://www.bleepingcomputer.com/news/security/singtel-qimr-berghofer-report-accellion-related-data-breaches/