GENERAL ANNOUNCEMENT::MEDIA STATEMENT RELATING TO ACCELLION FTA SECURITY INCIDENT

Issuer & Securities

Issuer/ Manager
SINGAPORE TELECOMMUNICATIONS LIMITED

Securities
SINGTEL - SG1T75931496 - Z74

Stapled Security
No

Announcement Details

Announcement Title
General Announcement

Date &Time of Broadcast
11-Feb-2021 07:30:24

Status
New

Announcement Sub Title
Media Statement relating to Accellion FTA Security Incident

Announcement Reference
SG210211OTHREAYP

Submitted By (Co./ Ind. Name)
Lim Li Ching (Ms)

Designation
Assistant Company Secretary

Description (Please provide a detailed description of the event in the box below)
Please see attachment.

Attachments

MS-20210211-Accellion.pdf

Total size =203K MB

Media Statement relating to Accellion's FTA Security Incident

Singtel has been informed by a third-party vendor Accellion that its file sharing system called FTA has been illegally attacked by unidentified hackers. This is a standalone system that we use to share information internally as well as with external stakeholders. Accellion has informed that this incident is part of a wider concerted attack against users of their file sharing system. (See attached press release from Accellion)

We have since suspended all use of the system and activated investigations, working closely with cyber security experts and the relevant authorities, including the Cyber Security Agency of Singapore which is providing additional guidance.

We are currently conducting an impact assessment with the utmost urgency to ascertain the nature and extent of data that has been potentially accessed. Customer information may have been compromised. Our priority is to work directly with customers and stakeholders whose information may have been compromised to keep them supported and help them manage any risks. We will reach out to them at the earliest opportunity once we identify which files relevant to them were illegally accessed.

This is an isolated incident involving a standalone third-party system. Our core operations remain unaffected and sound.

Singapore Telecommunications Limited
Company registration number: 199201624D
31 Exeter Road, Comcentre Singapore 239732
Tel: +65 6838 3388 Fax: +65 6732 8428
www.singtel.com

Press Release

ACCELLION PROVIDES UPDATE TO RECENT FTA SECURITY INCIDENT

All Known Vulnerabilities Closed and Migration Efforts Continue

Palo Alto, CA | February 1, 2021

Accellion, Inc., provider of the industry's first enterprise content firewall, today issued an update on the recently reported security incident regarding FTA, Accellion's legacy large file transfer product.

Accellion FTA, a 20 year old product nearing end-of life, was the target of a sophisticated cyberattack. All FTA customers were promptly notified of the attack on December 23, 2020. At this time, Accellion has patched all known FTA vulnerabilities exploited by the attackers and has added new monitoring and alerting capabilities to flag anomalies associated with these attack vectors.

Accellion kiteworks Content Firewall Unaffected

All vulnerabilities are limited exclusively to FTA. They do not in any way impact Accellion's enterprise content firewall platform known as kiteworks. The vast majority of Accellion's clients reside on the kiteworks platform, which is built on an entirely different code base, using state-of-the-art security architecture, and a segregated, secure development process.

In mid-December, Accellion was made aware of a zero-day vulnerability in its legacy FTA software. Accellion released a fix within 72 hours. This initial incident was the beginning of a concerted cyberattack on the Accellion FTA product that continued into January 2021. Accellion identified additional exploits in the ensuing weeks and rapidly developed and released patches to close each vulnerability. Accellion continues to work closely with FTA customers to mitigate the impact of the attack and to monitor for anomalies.

“Our latest release of FTA has addressed all known vulnerabilities at this time,” commented Frank Balonis, Accellion’s Chief Information Security Officer. “Future exploits, however, are a constant threat. We have encouraged all FTA customers to migrate to kiteworks for the last three years and have accelerated our FTA end-of-life plans in light of these attacks. We remain committed to assisting our FTA customers, but strongly urge them to migrate to kiteworks as soon as possible.”

FTA’s maturity notwithstanding, these exploits demonstrate a highly sophisticated attack. In 2021, every software security provider must not only demonstrate secure software architecture but must also be proficient at cyberwarfare. Accellion is uniformly committed to protecting its customers and their supply chain partners from cyber criminals by preventing breaches and compliance violations, rapidly responding to cyberattacks in process, and mitigating the impact of incursions with extensive forensics and customer support. In regard to this incident, Accellion is contracting with an industry-leading cybersecurity forensics firm to conduct a compromise assessment and will share their findings when available.

FTA customers are encouraged to contact Accellion customer support for additional information at support@accellion.com.

To learn more how the flagship Accellion kiteworks platform helps organizations secure their third party communications, please visit Enterprise Content Firewall.

About Accellion

The Accellion enterprise content firewall prevents data breaches and compliance violations from sensitive third party communications. With Accellion, CIOs and CISOs gain complete visibility, compliance and control over IP, PII, PHI, and other sensitive content across all third-party communication channels, providing secure email, secure file sharing, secure mobile file sharing, enterprise app and Microsoft Office plugins, secure web forms, secure file transfer like SFTP, and enterprise workflow automation. Accellion has protected more than 25 million end users at more than 3,000 global corporations and government agencies, including NYC Health + Hospitals; KPMG; Kaiser Permanente; National Park Service; Tyler Technologies; and the National Institute for