MINISTRY OF HEALTH
SINGAPORE

MH 6:01/5

MOH Advisory No. 02/2021

8 February 2021

Dear Licensees and Managers of PHMCA-Licensed Institutions

**CYBERSECURITY ADVISORY 2/2021 – CYBERSECURITY MEASURES IN RESPONSE TO SOLARWINDS SUPPLY CHAIN ATTACK**

SolarWinds, a US company that develops network management software, had confirmed in December 2020 that it fell victim to a highly sophisticated, supply chain attack which saw backdoors[1] inserted into software updates for its widely used Orion platform. These have been exploited to compromise many organisations globally, including reputable cybersecurity and technology companies such as FireEye, Microsoft and Cisco, as well as several healthcare providers in the US.

2. The Singapore Computer Emergency Response Team (SingCERT) has issued two alerts to update and guide the public on the implications of the SolarWinds supply chain attack and mitigating measures to undertake. **All licensees are strongly encouraged to review the SingCERT alerts attached at Annexes A1 and A2 together with this advisory, and work with your IT administrators or provider to review and implement the following cybersecurity measures:**

a. Confirm if you or your third party service providers are using SolarWinds Orion products, and deploy the recommended updates and patches as soon as possible (details at Annexes A1 and A2). If this is not possible, you are advised to consider disconnecting or powering down affected SolarWinds Orion products from your network.

**Cybersecurity Best Practice – Know Your Assets**

We recommend that an updated inventory of all hardware and software assets be regularly maintained, and that news on reported vulnerabilities and latest patches for these assets be regularly monitored, to minimise your

[1] Backdoors are covert methods of bypassing normal authentication or encryption safeguard used by attackers to secure persistent access to a targeted system.

Ministry of Health, Singapore
College of Medicine Building
16 College Road
Singapore 169854
TEL (65) 6325 9220
FAX (65) 6224 1677
WEB www.moh.gov.sg

exposure to malicious threat actors exploiting these vulnerabilities. This can be carried out by yourself or your IT provider.

b. Regardless of whether you are using SolarWinds Orion products, you are strongly encouraged to regularly monitor and review your application, system and network logs for any suspicious activities, and check your IT systems and network for any Indicators of Compromise (IOC) shared by compromised organisations whose products you are using. You should also encourage your third party service providers to do the same.

**Cybersecurity Best Practice – Close Monitoring of Privileged Accounts**

Administrator accounts grant their users privileged access with wide-ranging powers (e.g. accessing any file on the computer, changing security settings and installing software and hardware). Such accounts must be closely monitored as they are often exploited by attackers.

We recommend to keep a log of any changes to access rights for privileged accounts, and introduce a regime to review that any such changes are legitimate. Changes that cannot be confirmed to be legitimate warrant immediate further investigation and should be restored to its original configuration(s).

c. If there are any suspicious activities or signs of compromise, you are strongly encouraged to reset credentials (e.g. passwords), especially ones used by or stored in SolarWinds products.

**Cybersecurity Best Practice – Good Password Management**

In creating a strong password, it is good practice to use passphrases that combine at least four random words, avoid using the same password for multiple accounts and avoid using publicly known information as passwords.

d. If any IOCs are discovered, seek immediate professional cybersecurity expertise to help with incident response and recovery. If you are unsure where to seek such expertise, you can also contact and consult SingCERT at *(https://www.csa.gov.sg/singcert/reporting)* for assistance if required.

Ministry of Health, Singapore
College of Medicine Building
16 College Road
Singapore 169854
TEL (65) 6325 9220
FAX (65) 6224 1677
WEB www.moh.gov.sg

e. Subscribe to the SingCERT mailing list at *(https://www.csa.gov.sg/singcert/subscribe)* to keep abreast of latest cybersecurity alerts and advisories, and adopt recommended cybersecurity measures as appropriate to respond to fast-evolving cyber threats.

These measures are intended to help you safeguard your IT systems and electronic medical records, which are part of your obligations under the Private Hospitals and Medical Clinics Regulations (PHMCR) and the Personal Data Protection Act (PDPA).

3. Licensees are strongly encouraged to be vigilant against constant and evolving cybersecurity threats. With the recent spate of cyber-attacks on supply chains, licensees are also reminded to exercise strong oversight of technology risks in your arrangements with third party service providers to ensure the security and integrity of your IT systems and electronic medical records.

4. To further support licensees, the Ministry will be releasing a set of Cybersecurity Essentials in the coming quarter, with the objective of setting guidelines to help licensees improve the cybersecurity of your IT systems. More details will be released then.

5. If you have any questions or clarifications, please contact us at eLIS@moh.gov.sg.

Thank you.

A/PROF (DR) RAYMOND CHUA
GROUP DIRECTOR (HEALTHCARE REGULATION GROUP)
& ASSISTANT COMMISSIONER (CYBERSECURITY)
MINISTRY OF HEALTH

MS ANNIE LIM
MINISTRY CHIEF INFORMATION SECURITY OFFICER
MINISTRY OF HEALTH

Ministry of Health, Singapore
College of Medicine Building
16 College Road
Singapore 169854
TEL (65) 6325 9220
FAX (65) 6224 1677
WEB www.moh.gov.sg