IIROC OCRCVM
Investment Industry Regulatory Organization of Canada
Organisme canadien de réglementation du commerce des valeurs mobilières

IIROC NOTICE

Education Notice

Please distribute internally to:
Corporate Finance
Credit
Institutional
Internal Audit
Legal and Compliance
Operations
Registration
Regulatory Accounting
Research
Retail
Senior Management
Trading Desk
Training

Contact:
Suzanne Lasrado
Senior Manager, Financial & Operations Compliance
416-943-5880
slasrado@iiroc.ca

Ryan Li
Director, Information Security
416-943-5890
rli@iiroc.ca

IIROC Notice 20-0100
May 14, 2020

COVID-19 and Cybersecurity – Remote Access Services

This Notice is for IIROC Dealer Members who use remote access services (e.g. Virtual Private Network – VPN, remote desktop, etc.) to support work from home arrangements.

Over the last couple of months, IIROC has issued Notices to firms and to advisors and employees to alert them to increased cybersecurity threats related to the pandemic.

We continue to see evolving cybersecurity threats, this time related to the use of remote access services with attackers increasingly targeting and exploiting its vulnerabilities.

Background

Remote access service vendors have advised that potential vulnerabilities are being leveraged to gain access to internal networks of various organizations. Attackers have been observed actively scanning for vulnerable configurations. Once access is gained, attackers can remain undetected and will look to obtain additional privileges to launch future attacks such as ransomware or data exfiltration.

What to do?

Firms must continue to apply general security precautions and actions to all computing resources with vigilance to external facing components such as remote access services.

We strongly recommend that your Information Technology department or services provider does the following:

1) **Patch all systems** – ensure security patches and secure configurations are applied in a timely manner according to vendor recommendations.

2) **Monitor network environments** – continue to monitor your environment for any anomalous behaviour (e.g. brute force attacks, irregular login/network activity, etc.). Take immediate action including password resets for any suspected breaches.

3) **Implement multi-factor authentication (MFA)** – ensure MFA is implemented and enforced for all users when logging in from an external network.

4) **Install anti-virus/anti-malware solutions and updates** – ensure anti-virus/malware tools are in place and up to date with the latest indicators of compromise on servers, end points, and network.

Other resources

Further information and resources on managing cybersecurity threats, including guides and webinars, are available on IIROC's cybersecurity site.