Route1 Responds to Reported Citrix Hack

Toronto, March 11, 2019 - Route1 Inc. (OTCQB: ROIUF and TSXV: ROI) (the "Company" or "Route1"), North America's most advanced provider of industrial-grade data intelligence, user authentication and ultra-secure mobile workforce solutions, today responded to Friday's report from multiple news agencies that enterprise server, application and desktop virtualization provider Citrix has suffered a hack that may have led to stolen sensitive information about their technology as well as data of enterprises using their technology.

As reported in PC Magazine: "The FBI contacted Citrix about international cyber criminals breaking into the company's networks, Citrix revealed Friday. The feds told Citrix that the hackers likely broke in by successfully guessing the weak password to a company account using a tactic known as password spraying."

According to the US Department of Homeland Security, in a traditional brute-force attack, a malicious actor attempts to gain unauthorized access to a single account by guessing the password. This can quickly result in a targeted account getting locked-out, as commonly used account-lockout policies allow three to five bad attempts during a set period of time. During a password-spray, the malicious actor attempts a single password against many accounts before moving on to attempt a second password, and so on. This technique allows the actor to remain undetected by avoiding rapid or frequent account lockouts.

Password spray campaigns typically target single sign-on ("SSO") and cloud-based applications utilizing federated authentication protocols. An actor may target this specific protocol because federated authentication can help mask malicious traffic. Additionally, by targeting SSO applications, malicious actors hope to maximize access to intellectual property during a successful compromise.

In Friday's reported case, it is alleged that malicious actors used several compromised Citrix employee accounts to steal six, and possibly ten terabytes of data.

Our Response

Route1 maintains that password-based access to all systems and applications should be eliminated in favor of multi-factor authentication. The risk is exacerbated when weak authentication is used in conjunction with SSO. Certificate-based authentication relying on Public Key Infrastructure ("PKI") is the preferred method of implementing authentication. Smart card based authentication offers the highest degree of protection, and the federal government should only rely on PIV or CAC authenticated access for employees and contractors. Of particular concern is remote access where the attack surface is wide open.

Furthermore, Route1 maintains that allowing inbound communications to an enterprise network (via a VPN or other remote access solution approaches) creates multiple risk vectors for the enterprise. If it is going to be considered at all, it requires careful selection of the technology to be deployed, as many remote access solution providers treat security implementation as an after-thought. Route1's MobiKEY technology is a remote access technology that does not weaken the network perimeter. No open inbound ports is just one example of how the MobiKEY technology differs from the competition.

Additionally, if an enterprise is using Citrix to virtualize their desktops and then extend remote access to the virtualized desktop, Route1's MobiKEY should be deployed. MobiKEY will enhance the enterprise's security of their network and data, as well as deliver a complete user experience for the mobile worker.

MobiKEY is currently trusted by the U.S. government and enterprise security teams to secure external access to their Citrix VDI installations. MobiKEY is a proven solution to increase an enterprise's security posture. MobiKEY enhances a Citrix deployment for remote access as follows:

- Delivers simplified access to VDI resources for end-users as the MobiKEY solution is completely portable.
- Provides access to VDI resources without the need for government or enterprise furnished equipment, delivering a rapid return on investment.
- For the U.S. Government, MobiKEY provides integrated HSPD-12 compliant PIV and CAC based user authentication.
- There is no edge gateway, eliminating the risk of penetration attacks.
- Mitigates risk from remote endpoint malware.
- Route1's MobiKEY technology is designed to protect from data leakage.
- Seamlessly integrates with Citrix VDI, there are multiple deployment models available.
- Eliminates the need for a VPN to connect remote users - associated risks removed in using a VPN. MobiKEY is the un-VPN.
- Minimal learning curve for end-users compared to traditional Citrix VDI deployments which will reduce help desk calls and deployment costs.
- Enhances the overall end-user experience.

Citrix is an American multinational software company that provides server, application and desktop virtualization, networking, software as a service, and cloud computing technologies.

About Route1 Inc.

Route1, operating under the trade name **GroupMobile**, is North America's most advanced provider of industrial-grade data intelligence, user authentication, and ultra-secure mobile workforce solutions. The Company helps all manner of organizations, from government and military to the private sector, to make intelligent use of devices and data for immediate process improvements while maintaining the highest level of cyber security. Route1 is listed on the OTCQB in the United States under the symbol

ROIUF and in Canada on the TSX Venture Exchange under the symbol ROI. For more information, visit: www.route1.com.

For More Information, Contact:
Tony Busseri
Chief Executive Officer, Route1 Inc.
+1 416 814-2635
tony.busseri@groupmobile.com

This news release, required by applicable Canadian laws, does not constitute an offer to sell or a solicitation of an offer to buy any of the securities in the United States. The securities have not been and will not be registered under the United States Securities Act of 1933, as amended (the "U.S. Securities Act") or any state securities laws and may not be offered or sold within the United States or to U.S. Persons unless registered under the U.S. Securities Act and applicable state securities laws or an exemption from such registration is available.

Neither the TSX Venture Exchange nor its Regulation Services Provider (as that term is defined in the policies of the TSX Venture Exchange) accepts responsibility for the adequacy or accuracy of this release.

# # #