Kiteworks (formerly Accellion) CISO Offers Advice to Customers Impacted by Fortra GoAnywhere's MFT Breach

Doing four things means the difference between weathering or faltering after a supply chain breach.

SAN MATEO, CA, USA, February 7, 2023 /EINPresswire.com/ -- Kiteworks, which delivers data privacy and compliance for sensitive content communications through its Private Content Network, which includes a Managed File Transfer offering, released four recommendations from its CISO and SVP of Operations, Frank Balonis, for Fortra's GoAnywhere MFT customers impacted by a zero-day remote code injection exploit in its managed file transfer (MFT).

> "Minimizing the damage and risk of a zero-day attack requires speed and a software vendor that institutes often the right mitigation measures."
>
> *Frank Balonis*

The exploit requires access to the administrative console of GoAnywhere MFT, which in most cases is accessible only from within a virtual private network (VPN) or by allow-listed IP services running in cloud environments like AWS or Azure. The potential supply chain damage resulting from the vulnerability is relegated to GoAnywhere MFT customers that have exposed their administrative console to the internet (151 per Kevin Beaumont who performed a Shodan scan).

Frank Balonis led the response effort when he experienced a similar zero-day vulnerability of Accellion's legacy File Transfer Appliance (FTA) about two years ago and worked in lockstep with Mandiant for incident response. Seeking to provide Fortra GoAnywhere MFT customers with lessons learned based on those he observed when helping Kiteworks customers enact an effective incident response plan, Balonis has four recommendations for GoAnywhere MFT customers:

1. Implement Patches as Soon as They Are Available. As of the date of this release, GoAnywhere had not released patches for the vulnerability. However, as soon as they are available, GoAnywhere customers should implement them as quickly as they can.

2. Listen to GoAnywhere. Whenever a software provider experiences a zero-day vulnerability, it is extremely important for customers to listen to the vendor and follow their instructions for mitigating configurations. For example, as Fortra instructed its customers, internet port access to

the administrative console of GoAnywhere MFT should be shut off immediately.

3. Clearly Define Your Communication Channels. You need to designate everyone within your organization who needs to be included on communications with the GoAnywhere MFT team and ensure that list is communicated to them. This list should include names, contact information, and roles and responsibilities.

4. Follow Best Practices. Software vendors provide customers with best practices, and it is important to follow them. It is also important for organizations to adhere to their own security best practices. In the case of the GoAnywhere MFT vulnerability, Fortra advised customers not to expose their administrative console to the public internet but rather to access it through VPN or IP-enabled cloud service. As Fortra is likely seeing advanced persistent behavior that includes the creation of new administrative accounts and users, Fortra also is telling customers to review all administrative users and monitor for unrecognized usernames, especially those created by "system."

"Minimizing the damage and risk of a zero-day attack requires speed and a software vendor that institutes often the right mitigation measures," said Balonis. "GoAnywhere MFT customers need to ensure they have the right communication channels established with Fortra and follow directions they receive, including implementing patches quickly. And because of the advanced persistent nature of many cyberattacks today, GoAnywhere MFT customers need to ensure they are adhering to security best practices—both those they themselves have in place as well as those from Fortra—to ensure additional access points are not developed."

Following Accellion's FTA breach, Accellion retained over 90% of its customers by migrating to the company's Kiteworks Private Content Network (PCN) offering. This shows how outstanding care and diligence throughout the lifecycle of an incident can make the difference between emerging from a breach stronger or weaker as a company. Today, the Kiteworks PCN is one of the most security-hardened platforms on the market, and Kiteworks had the strongest year of growth in the history of the company in FY22.

For additional details on the GoAnywhere MFT zero-day vulnerability and recommendations to GoAnywhere MFT customers, read our blog post.

About Kiteworks
Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and save of sensitive content. The Kiteworks platform provides customers with a Private Content Network that delivers content governance, compliance, and protection. The platform unifies, tracks, controls, and secures sensitive content moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all sensitive content communications. Headquartered in Silicon Valley, Kiteworks protects millions of end users for thousands of global enterprises and government agencies.

Patrick Spencer
Kiteworks
email us here
Visit us on social media:
Facebook
Twitter
LinkedIn
YouTube
