Updates
March 07, 2022

FCC Examines Cybersecurity Vulnerabilities Following Russian Invasion of Ukraine

The U.S. Federal Communications Commission (FCC) published a Notice of Inquiry (NOI) on February 28, 2022, inviting public comment on vulnerabilities that threaten the security and integrity of the Border Gateway Protocol (BGP), which is central to the internet's global routing system. BGP's initial design is widely deployed and lacks security features to ensure trust in the information being exchanged. The NOI seeks comment on steps the FCC can take to help protect and strengthen the nation's communications network and other critical infrastructure, and it represents the first major cybersecurity-related action taken by the FCC in the wake of Russia's escalating military campaign in Ukraine.

Background

The FCC plays a key role in protecting the security of communications and other critical infrastructure in the United States. Among other things, the FCC is charged under the Communications Act of 1934 with seeking "maximum effectiveness from the use of radio and wire communications in connection with the safety of life property."

As a backbone technology of the global internet, the BGP is a key component of the security framework. The BGP is a protocol for exchanging routing and reachability information between independently managed networks on the internet. The protocol was originally designed in 1989 and received its most recent major update in 2006. During that time, there were only a few independently managed networks and those networks generally "trusted" each other. Thus, the protocol did not originally include security features for ensuring the trustworthiness of information exchanged using it.

Although there have been some recent developments—such as the Resource Public Key Infrastructure (RPKI) to improve BGP's security—today, bad actors may deliberately falsify reachability information that the BGP uses to influence the path of internet traffic, such as by forcing traffic through a specific network or prevent it from reaching the intended destinations. These "BGP hijacks" can be used for a variety of nefarious purposes, from stealing personal information to state-level espionage. Russian network operators in particular have been suspected of BGP hijacking, which is an especially salient issue given Russia's recent invasion of Ukraine and the specter of potential cyberattacks being conducted as part of the conflict. Importantly, the FCC has also recently announced that it has begun reviewing media and telecom companies for Russian ownership ties. This suggests that the FCC may be poised to take actions against any media and telecom companies with extensive ties to the Russian government and military, as it has against Chinese government-affiliated telecoms.

Notice of Inquiry

In light of these concerns, the FCC seeks comment on how it can best help protect the nation from the BGP's vulnerabilities and facilitate implementation of industry standards and best practices that would help mitigate the potential harms of these vulnerabilities. The FCC wants to better understand the BGP ecosystem, including the extent to which network operators use the BGP and have deployed BGP security measures, such as RPKI. The

FCC seeks comment on the effectiveness of these security measures in preventing BGP hijacking.

The FCC also seeks comment on potential normative concerns surrounding BGP vulnerabilities and security measures. Specifically, the FCC wants to know how its proposals may promote or inhibit advances in diversity, equity, inclusion, and accessibility. Additionally, the FCC has asked the public to weigh in on potential costs of implementing BGP security measures, such as hardware expenditures and the benefits of having more secure internet routing, including national security, economic, and public safety.

Initial comments will be due 30 days after the NOI is published in the Federal Register and reply comments will be due 30 days after the initial comment deadline.

Authors

Marc S. Martin

Partner
MMartin@perkinscoie.com 202.654.6351

Tyler D. Robbins

Associate
TRobbins@perkinscoie.com 202.654.3313

Explore more in

Technology Transactions & Privacy Law Privacy & Security Communications Fintech

Related insights

Update

Employers and Immigration Under Trump: What You Need To Know

Update

‘Tis the Season… for Cybercriminals: A Holiday Reminder for Retailers