

Media Contact:

MediaRelations@fcc.gov

For Immediate Release

FCC PROPOSES REPORTING REQUIREMENTS TARGETED TO IMPROVING INTERNET ROUTING SECURITY

Broadband Providers Would Create BGP Security Plans and Largest Providers Would Also File Quarterly Reports on BGP Risk Mitigation Progress

WASHINGTON, June 6, 2024—The Federal Communications Commission today proposed action to help protect America’s communications networks against cyberattacks by improving internet routing security. The Commission’s proposal would require broadband providers to create confidential reports on the steps they have taken, and plan to undertake, to mitigate vulnerabilities in the Border Gateway Protocol (BGP), the technical protocol used to route information across the internet. The nation’s largest broadband providers would also be required to file specific public data on a quarterly basis demonstrating their BGP risk mitigation progress. Today’s proposal would promote more secure internet routing and provide the Commission and its national security partners with up-to-date information on this critical issue.

BGP’s initial decades-old design, which remains widely deployed today, does not include intrinsic security features to ensure trust in the information that is relied upon to exchange traffic among independently managed networks on the internet. BGP national security experts have raised concerns that a bad network actor may deliberately falsify BGP reachability information to redirect traffic. These “BGP hijacks” can expose Americans’ personal information; enable theft, extortion, and state-level espionage; and disrupt services upon which the public or critical infrastructure sectors rely.

To help address these vulnerabilities, the Commission today adopted a Notice of Proposed Rulemaking proposing that:

- Broadband internet access service providers prepare and update confidential BGP security risk management plans at least annually. These plans would detail their progress and plans for implementing BGP security measures that utilize the Resource Public Key Infrastructure (RPKI), a critical component of BGP security.
- The nine largest broadband providers file their BGP plans confidentially with the Commission as well as file quarterly data available to the public that would allow the Commission to measure progress in the implementation of RPKI-based security measures and assess the reasonableness of the BGP plans. These large providers would not have to file subsequent detailed plans with the Commission if they met a certain security threshold.
- Smaller broadband providers would not be required to file their plans with the Commission but rather make them available to the Commission upon request.

The Commission is seeking public comment on these proposals and other measures related to implementing RPKI-based security. In taking today's action, the Commission recognized the efforts of multiple stakeholders over the past twenty years to address BGP vulnerabilities but noted that more work needs to be done to secure internet routing, which is critical to public safety and national security.

Action by the Commission June 6, 2024 by Notice of Proposed Rulemaking (FCC 24-62). Chairwoman Rosenworcel, Commissioners Carr, Starks, Simington, and Gomez approving. Chairwoman Rosenworcel and Commissioner Starks issuing separate statements.

PS Docket Nos. 24-146, 22-90

###

Media Relations: (202) 418-0500 / ASL: (844) 432-2275 / Twitter: @FCC / www.fcc.gov

This is an unofficial announcement of Commission action. Release of the full text of a Commission order constitutes official action. See MCI v. FCC, 515 F.2d 385 (D.C. Cir. 1974).