Lumen® DDoS Mitigation Services

Frequently asked questions about RPKI
December 2021

Customers that use Lumen DDoS Mitigation Service need to be aware of the impact of resource public key infrastructure (RPKI). Your DDoS service schedule with Lumen states that customers who have published RPKI ROAs are responsible for updating the route registry associated with their IP space and AS number to permit Lumen to advertise the applicable IP address to help ensure proper routing of legitimate traffic. If you don't update the registry accordingly, Lumen's ability to mitigate some or all the attack(s) on your IP address will be reduced*.

You need to take specific action to ensure DDoS Mitigation can properly direct traffic to scrubbing centers when needed.

Why is resource certification necessary?

The internet infrastructure was built based on mutual trust between service providers to ensure advertised routes are safe, accurate and will not be maliciously altered. Although that model proved sufficient in the earlier days for internet development, it has become increasingly vulnerable to configuration mistakes or abuse and attack by malicious actors looking to redirect routes to achieve criminal goals. This is called BGP hijacking or IP hijacking.

Resource certification enables IP holders to specify which autonomous systems (AS) are authorized to originate their IP prefixes in BGP announcements. IP service providers can validate IP route announcements at peering points to ensure that announcements were originated by the AS authorized to do so and drop routes that come from unauthorized sources.

What is RPKI and how does it help?

RPKI enables IP address holders to specify which autonomous systems are authorized to originate their IP address prefixes. RPKI is a standard set of protocols and services defined by The IETF (Internet Engineering Task Force) beginning with RFC 6840, "An Infrastructure to Support Secure Internet Routing," and a dozen or so supporting RFCs. Using cryptographically verifiable statements, RPKI helps to ensure that internet IP address resource holders are certifiably linked to those resources, and reliable routing origin data is available upon which to base routing decisions.

Customers create the association between IP addresses and agencies that are permitted to originate BGP announcements for those IP address by filing a route origin authorization (ROA) with and authorized registry.

Do all internet service providers support RPKI?

Lumen supports RPKI and most service providers are transitioning to it as well. For an updated list of internet service providers supporting RPKI, see https://IsBgpSafeYet.com.

What is the impact to Lumen DDoS Mitigation customers?

To redirect IP traffic to DDoS scrubbing centers, Lumen makes BGP route announcements for IP addresses that need to be routed to scrubbing centers. If these IP addresses are registered via RPKI and Lumen does not have a route origin authorization (ROA) to originate advertisements for the DDoS protected IP address space using Lumen autonomous systems, then service providers that are enforcing RPKI will drop the route announcement. This means that some or all traffic, depending on which path the traffic takes from the originator to the protected infrastructure, will not redirected to and mitigated by Lumen DDoS Mitigation.

When does DDoS Mitigation route traffic to DDoS scrubbing centers?

There are several DDoS Mitigation Services that determine when and how the traffic is routed to scrubbing centers. The table below addresses tis question.

Service	IP traffic redirection
Always on	IP address space is directed through the scrubbing centers all the time.
On demand	IP address space is directed through the scrubbing centers only when under an active DDoS attack.

Do all DDoS Mitigation customers need to take action?

No, customers that are using IP addresses that meet the following criteria need to take action:

- Customers that hold their own IP addresses and have registered them with RPKI.
- Customers that are using IP addresses held by another agency who have registered them with RPKI.

What action needs to take place?

Contact your internet numbering registry to file a route-origin authorization (ROA) to designate Lumen as an authorized agency to originate BGP route updates for your IP addresses. Information needed for this ROA includes:

- Customer-held public IP addresses
- Lumen ASNs: 3356, 202, and 203
- Customer supplied public key (as all communication will be encrypted)
- The date range that this association should be active

Information required may vary, depending on the registry. Contact the same registry that you originally registered your IP Addresses with RPKI. Internet number registries are regional:

- ARIN: North American (https://www.arin.com)
- RIPE: Europe (https://www.ripe.net)
- APNIC: Asia Pacific (https://www.apnic.com)
- LACNIC: Latin America and Caribbean nations (https://lacnic.net)
- AFRINIC: Africa (https://www.afrinic.net)

Can Lumen file the ROA on my behalf?

The actual holder of the IP addresses needs to file the ROA. This is to prevent fraudulent filings and to ensure the fidelity of the registration data.

Where can I go for additional information?

The following resources provide additional information free of charge:

- The Internet Engineering Task Force (IETF): https://ietf.org
- RFC 6480 from IETF: https://tools.ietf.org/html/rfc6840
- The numbering registry agents listed above
- Is BGP Safe Yet: https://IsBgpSafeYet.com
- Lumen Security Operations Center (SOC): soc@lumen.com

* DISCLAIMER: This information is provided for informational purposes only. It is not intended to amend any contractual terms between Lumen and customer. The DDoS Service is a supplement to customer's existing security and compliance frameworks, network security policies and security response procedures, for which Lumen is not, and will not be, responsible.