https://securityintelligence.com/news/biden-harris-administration-releases-roadmap-enhance-internet-routing/

Biden-Harris administration releases roadmap to enhance internet routing

October 15, 2024By Sue Poremba

The Biden-Harris Administration has taken another step toward improving the nation's cybersecurity. In September, the White House Office of the National Cyber Director (ONCD) announced it was putting policies in place to address a key security vulnerability associated with the Border Gateway Protocol (BGP).

BGP is a set of rules that helps the internet work by selecting the best route for data to travel between networks. It is a fundamental protocol that allows networks to communicate with each other. However, it is susceptible to misconfigurations that lead to exploits by malicious actors.

“Securing BGP is essential to safeguarding the integrity of our digital infrastructure. Through strong partnerships — both with industry and with government agencies — we can enhance the resilience of our internet routing, ensuring a secure and reliable

internet for our nation,” said CISA Director Jen Easterly, in a statement announcing the Roadmap to Enhancing Internet Routing Security.

The need to address security in BGP

The interconnectedness of the internet and cloud computing means that an outage or a software exploit for one company could snowball to other organizations. It’s what happened with a Cloudflare outage five years ago. When Cloudflare was impacted by a bad software deployment, its customers were also impacted by the problem, all because of the connected relationships through BGP.

ONCD, in collaboration with CISA, recommended actions designed to apply to all network types, meaning all network service providers and entities that operate enterprise networks or hold their own IP address resources. They are, briefly:

- Risk-based planning
- ROA publication
- Contracting requirements
- Monitoring
- Understanding the basic problem of BGP

Let’s use an analogy, said Stuart Madnick, Professor of Information Technology at the MIT Sloan School of Management, in email commentary. Consider your car’s GPS. It indicates which roads are crowded (usually shown in red) and tries to route you around them.

But how does your GPS know which roads are crowded? It relies on information from various sources — what if these sources are lying?
“The internet operates the same way,” explained Madnick. “The internet uses various sources to route its traffic, including gateways. In simple terms, the gateways provide traffic information such as ‘the way to get to Boston is to take this road — I am the gateway.’”

It’s a problem in internet architecture because internet traffic could then be routed to places where it might be intercepted or modified. “This has actually happened a couple of times in the past, though it was claimed to be an accident,” said Madnick.
What is groundbreaking about the roadmap

The internet (and its predecessors) were based on the notion that all its components were cooperative and trustworthy. To the extent that these assumptions need to change, it is a “game changer.”

“I have not studied the details of the proposal, but it will likely change the nature of the internet as we know it,” said Madnick. “Just as China has prevented the free flow of internet traffic in and out of its country, this could further fragment the internet or reduce its efficiency and resiliency. The outcomes are likely not well understood in advance, and possible unintended consequences could result.”

As for the White House, the goals are clear.

“Internet routing security is a vital part of network security that, when overlooked, can lead to loss of service, theft of data and other malicious attacks,” Assistant Secretary of Commerce for Communications and Information and NTIA Administrator Alan Davidson, said in a formal statement. “ONCD’s roadmap is an important step towards helping the entire internet ecosystem protect users from these threats.”