ultraviolet

CONFIDENTIAL

THREAT REPORT:

CISPA Researchers Document New DoS Attack - Loop Dos

Services Performed By:
UltraViolet Cyber
Johnathon Moyer
(443) 351-7630
info@uvcyber.com

Published Date:
04/10/2024

Contents

1 Executive Summary

The ‘Loop DoS’ attack generally follows this pattern: a threat actor identifies two DNS resolvers with a configuration which causes the servers to respond to messages with an error message of their own. The threat actor then sends a specifically crafted error message with a resolve answer included. This will tell DNS resolver A to send error messages back to resolver B. Resolver B will then respond to the error message with an error message of its own and send that back to resolver A. This will continue in a loop until the resolvers crash or network administrators notice the traffic and work to resolve the feedback loop. Because this attack vector can be stacked, many loops may be active at the same time. This could theoretically take up all available sockets and block any legitimate incoming traffic, triggering a denial of service (DoS) attack.

2 Technical Analysis

The details of the attack have not yet been published, as the attack vector has not yet been observed in the wild. However, monitoring network traffic for increases in overall volume, with particular attention for modern UDP application-layer protocols 'TFTP', 'DNS' and 'NTP', and legacy UDP protocols 'QOTD/RFC865', 'Chargen/RFC864', 'Echo/RFC862', 'Time', 'Daytime' and 'Active Users', may help identify this attack. The listed legacy protocols have this vulnerability included by design.

These application-layer loops are different from normal misconfiguration issues from network-layer loops. Time-to-live hop limits in IP detections would not mitigate the application-layer specific attack. While all attributes related to this vulnerability have not yet been researched, a common trend appears to relate some of the vulnerability to pre-2010 versions of ntpd.

Disclosures to affected vendors and developers of products vulnerable to this new attack will be sent out over time. Shadowserver sent a report related to these vulnerable services to organizations already subscribed to their service back on December 20, 2023. Regular organizations can protect themselves against this attack vector by ensuring their web-facing services are behind a firewall and that affected services and their ports are reassigned to ephemeral ports rather than the standard ports. When the error messages are sent to ephemeral ports instead, the loop cannot occur anymore.

3 What Ultraviolet Cyber is Doing

- Ultraviolet Cyber regularly updates our IoC database to ensure alerting is up to date
- Monitoring commands that are associated with malicious activity from threat actors
- Monitoring network logs for traffic to known malicious sites

4 What Customers Can Do

- Update or isolate vulnerable applications
- Restrict access to impacted services by utilizing ephemeral ports. This breaks the communication loop, as the vulnerability maps communication to known associated ports for the given service. You can use reverse proxies or filter non-ephemeral source ports towards their respective servers.

5 References

CISPA (2024, March 19). *Loop DoS: New Denial-of-Service attack targets application-layer protocols*. Retrieved March 29, 2024, from https://cispa.de/en/loop-dos

Dogan, N. (2024, January 7). *Discovering Network Loops (Layer 2) with Wireshark*. Retrieved March 29, 2024, from https://www.golinuxcloud.com/discovering-network-loops-with-wireshark/

Rossow, C., & Pan, Y. (2024, March 26). *Advisory on Application-layer Loop DoS Attacks*. Google Docs. Retrieved March 29, 2024, from https://docs.google.com/document/d/1KByZzrdwQhrXGPPCf9tUzERZyRzg0xOpGbWoDURZxTI/edit

Toonk, A. (2024, March 13). *The Risks and Dangers of Amplified Routing Loops.* Retrieved March 29, 2024, from https://toonk.io/the-risks-and-dangers-of-amplified-routing-loops/index.html