March 21, 2024

Loop DoS: Datagram Application-Layer Denial of Service Attacks

On March 19, 2024, the research group of Prof. Dr. Christian Rossow at CISPA Helmholtz Center for Information Security in Germany disclosed a new attack vector that exploits a common vulnerability in application-layer services based on the User Datagram Protocol (UDP). The vulnerability in several implementations of UDP application protocols is tracked through CVE-2024-2169.

Attack Vector

Attackers could potentially craft a payload that triggers an error condition in a vulnerable server resulting in a reply with a failure datagram. The server failure datagram, when received by another vulnerable server, will result in a subsequent server failure datagram to the first vulnerable server. When both vulnerable systems keep sending error messages to each other indefinitely, the loop condition becomes perpetual. Since datagrams are regenerated for every response, the IP Time-to-Live (TTL) hop count limiter does not alter the indefinite nature of the loop condition.

To initiate a loop on a target system, an attacker needs to identify at least one other vulnerable system that runs the same service and can reach the targeted service. By spoofing the source IP of the initial request, an attacker can trick its victim into responding to another vulnerable server. The attack can be amplified by creating multiple loops between two vulnerable systems and by adding more (other) vulnerable systems and establishing enough perpetual loops to overload the victim.

Affected Services

The vulnerability was identified in several hundreds of thousands of publicly exposed servers running vulnerable implementations of DNS, TFTP, NTP, Echo, Chargen or QOTD. The researchers focused on those applications that are most widely deployed. The vulnerabilities in NTP can likely be attributed to systems that use a version of ntpd that predates 2010. The legacy protocols Echo, Chargen, QOTD, Time, Daytime and Active Users were discovered to be vulnerable by design. TFTP and DNS are still under research and require more input from operators of vulnerable systems to discover the exact nature of the vulnerability.

Reasons for Concern

Because of its stateless character, UDP allows legitimate services to be abused for volumetric amplification DDoS attacks and now also loop DoS attacks. The researchers estimated that 300,000 internet hosts are vulnerable to loop DoS.

The loops consist of single packet datagrams and generate a flood to the victim that originates from the same IP and UDP port. Per IP packet rate detectors should be able to detect such loop conditions. Depending on the actual number of vulnerable systems, the attack could be distributed across multiple servers resulting in an attack that is harder to detect based on per IP packet rates. The estimated number of vulnerable hosts per service exposed on the internet, as provided by the researchers, provides a good measure for the risk of distributed loop attacks associated with a specific service (see Table 1).

Table 1: Estimated number of vulnerable hosts on the internet (per service)

Service	Estimated vulnerable hosts
NTP	89k
DNS	63k
Echo (RFC862)	56k
TFTP	23k
Chargen (RFC864)	22k
QOTD (RFC865)	21k

Detecting Vulnerable Systems

The researchers at CISPA published a tool to scan and discover systems that are vulnerable to the attack payloads they have been able to identify. Attack payloads for DNS, TFTP and NTP are defined in the 'simple_verify.py' Python script.

Recommendations

If possible, avoid exposing services based on UDP and more specifically any of the services listed in Table 1. When there is a need to expose one of those services, ensure it is kept up to date with the latest security patches and protected by adequate solutions to prevent abuse and detect anomalous behavior.

The researchers at CISPA Helmholtz Center for Information Security in Germany are updating their advisory as more information becomes available.

Indicators of Compromise (IoC)

- CVE-2024-2169
- Hex versions of DNS, TFTP and NTP payloads that can trigger the loop condition are provided in the file 'simple_verify.py' on the CISPA GitHub.

EFFECTIVE DDOS PROTECTION ESSENTIALS

Hybrid DDoS Protection – Use on-premise and cloud DDoS protection for real-time DDoS attack prevention that also addresses high-volume attacks and protects from pipe saturation

Behavioral-Based Detection – Quickly and accurately identify and block anomalies while allowing legitimate traffic through

Real-Time Signature Creation – Promptly protect against unknown threats and zero-day attacks

A Cybersecurity Emergency Response Plan – Turn to a dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks

Intelligence on Active Threat Actors – High fidelity, correlated and analyzed data for preemptive protection against currently active known attackers

For further network and application protection measures, Radware urges companies to inspect and patch their network to defend against risks and threats.

EFFECTIVE WEB APPLICATION SECURITY ESSENTIALS

Full OWASP Top-10 coverage against defacements, injections, etc.

Low false positive rate using negative and positive security models for maximum accuracy

Auto-policy generation capabilities for the widest coverage with the lowest operational effort

Bot protection and device fingerprinting capabilities to overcome dynamic IP attacks and achieve improved bot detection and blocking

Securing APIs by filtering paths, understanding XML and JSON schemas for enforcement, and using activity tracking mechanisms to trace bots and guard internal resources

Flexible deployment options including on-premises, out-of-path, virtual or cloud-based

LEARN MORE AT RADWARE'S SECURITY RESEARCH CENTER

To know more about today's attack vector landscape, understand the business impact of cyberattacks, or learn more about emerging attack types and tools, visit Radware's Security Research Center. Additionally, visit Radware's Quarterly DDoS & Application Threat Analysis Center for quarter-over-quarter analysis of DDoS and application attack activity based on data from Radware's cloud security services and threat intelligence.

THIS REPORT CONTAINS ONLY PUBLICLY AVAILABLE INFORMATION, WHICH IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. ALL INFORMATION IS PROVIDED “AS IS” WITHOUT ANY REPRESENATION OR WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES THAT THIS REPORT IS ERROR-FREE OR ANY IMPLIED WARRANTIES REGARDING THE ACCURACY, VALIDITY, ADEQUACY, RELIABILITY, AVAILBILITY, COMPLETENESS, FITNESS FOR ANY PARTICULAR PURPOSE OR NON-INFRINGEMENT. USE OF THIS REPORT, IN WHOLE OR IN PART, IS AT USER’S SOLE RISK. RADWARE AND/OR ANYONE ON ITS BEHALF SPECIFICALLY DISCLAIMS ANY LIABILITY IN RELATION TO THIS REPORT, INCLUDING WITHOUT LIMITATION, FOR ANY DIRECT, SPECIAL, INDIREC, INCIDENTAL, CONSEQUENTIAL, OR EXAMPLARY DAMAGES, LOSSES AND EXPENSES ARISING FROM OR IN ANY WAY REALTED TO THIS REPORT, HOWEVER CAUSED, AND WHETHER BASED ON CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHER THEORY OF LIABILITY, EVEN IF IT WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, LOSSES OR EXPENSES.