← Back to Blog

ORIGINAL RESEARCH Jan 6, 2026 12 min read CVE-2024-45163

CVE-2024-45163: How Our Team Discovered a Kill Switch in the Mirai Botnet

CVE ID	CVE-2024-45163
CVSS SCORE	9.1 CRITICAL (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H)
AFFECTED SOFTWARE	Mirai botnet CNC server (all known variants through August 19, 2024)
VULNERABILITY TYPE	CWE-400: Uncontrolled Resource Consumption
ATTACK VECTOR	Network: no authentication, no user interaction required
IMPACT	Remote denial of service against botnet command-and-control infrastructure
DISCOVERED BY	Flowtriq Research Team
NVD ENTRY	nvd.nist.gov/vuln/detail/cve-2024-45163

The Discovery

Mirai is the most prolific DDoS botnet in history. Since its source code was released publicly in 2016, it has spawned hundreds of variants that collectively power the majority of DDoS-for-hire services and botnet operations worldwide. It has been responsible for some of the largest DDoS attacks ever recorded, including the 2016 Dyn DNS attack that took down Twitter, Netflix, and Reddit simultaneously.

Our research team spends significant time studying botnet infrastructure: not just to detect the attacks they produce, but to understand how the botnets themselves operate. During a routine analysis of Mirai's CNC (command-and-control) server source code, we identified a critical flaw in how the server handles incoming TCP connections during the pre-authentication phase.

The vulnerability is deceptively simple: the CNC server does not properly manage concurrent connections that have initiated but not completed authentication. By opening a large number of simultaneous TCP connections and sending a recognized username (like `root`) without completing the authentication handshake, an attacker can exhaust the server's resources, causing it to crash.

> In practical terms, this means anyone with a basic script and a single-core VPS can take down a Mirai command-and-control server. The botnet operator's entire fleet of compromised IoT devices becomes disconnected and unable to receive attack commands.

Technical Breakdown

How Mirai's CNC Authentication Works

When a bot (infected device) or operator connects to a Mirai CNC server, the server initiates a simple telnet-like authentication flow:

1. The server accepts the TCP connection
2. The server sends a username prompt

3. The client sends a username
4. The server sends a password prompt
5. The client sends a password
6. The server validates credentials and either grants or denies access

The critical design flaw is in step 3. When the CNC server receives a username, it allocates resources for that session and holds the connection open, waiting for the password. There is no timeout, no connection limit per source IP, and no cap on the total number of concurrent pre-authenticated sessions.

The Exploit

The attack is straightforward:

```
// Simplified exploit logic (pseudocode)
for i in range(0, 10000):
    conn = tcp_connect(cnc_server, cnc_port)
    conn.send("root\n")
    // Do NOT send password. Hold connection open.
    connections.append(conn)

// Server runs out of file descriptors / memory
// CNC crashes. All bots disconnect.
```

Each connection sends a valid username but never completes authentication. The CNC server holds each of these connections open indefinitely, allocating memory and file descriptors for each one. After several thousand connections, the server exhausts its resources and crashes.

The key characteristics that make this vulnerability critical:

> **No authentication required.** The exploit works in the pre-authentication phase. The attacker does not need any credentials.

Trivially exploitable. The proof of concept runs on minimal hardware: a single-core VM with 1GB RAM is sufficient to crash a CNC server.

Affects all known Mirai variants. Because the flaw is in the original CNC source code that every variant inherits, it affects the entire Mirai ecosystem.

No network amplification needed. Unlike DDoS attacks that require botnets or amplification, this exploit works directly from a single source.

Why This Wasn't Caught Before

Mirai's source code has been public since 2016, analyzed by hundreds of security researchers, and dissected in countless academic papers. So why did this vulnerability go unnoticed for eight years?

The answer is that most security research on Mirai focuses on the *bot* side: how it infects devices, how it receives commands, and how it generates attack traffic. The CNC server is treated as a black box that operators set up and forget. Very few researchers spend time auditing the CNC's connection handling under adversarial conditions, because the CNC is typically seen as "the attacker's problem."

Our perspective was different. As a DDoS detection company, we are interested in every possible way to disrupt the infrastructure that generates attacks. When we examined the CNC source code with that lens, looking for weaknesses in the attacker's infrastructure, not the victim's, the vulnerability became apparent.

Impact and Implications

For Defenders and Law Enforcement

CVE-2024-45163 provides a practical tool for disrupting active Mirai botnet operations. When a Mirai CNC server is crashed using this vulnerability, every bot connected to that server loses its command channel. The bots remain infected but cannot receive new attack instructions until the operator restarts the CNC and the bots reconnect.

This has significant implications for:

Law enforcement takedowns. Agencies conducting botnet disruption operations can use this vulnerability to quickly disable CNC servers without needing to seize the underlying infrastructure.

Active defense. Organizations under active DDoS attack from a Mirai variant can potentially disrupt the attack by targeting the CNC server, cutting off the attacker's ability to direct the botnet.

ISP and hosting provider response. Providers who identify Mirai CNC servers operating on their infrastructure can neutralize them while preparing formal abuse action.

For Botnet Operators

The vulnerability exposes a fundamental architectural weakness in Mirai's design. Botnet operators could mitigate it by implementing:

- Connection rate limiting per source IP
- Maximum concurrent pre-authenticated session caps
- Idle timeouts for connections that send a username but no password
- File descriptor limits on the CNC process

However, because Mirai variants are typically operated by unsophisticated actors using copy-pasted source code, the vast majority of active CNC servers are unlikely to be patched. This vulnerability will remain exploitable across the Mirai ecosystem for years.

Why This Matters for DDoS Defense

Mirai and its variants remain one of the largest sources of DDoS attack traffic globally. Cloudflare's 2025 DDoS reports continued to flag Mirai-generated attacks as a persistent threat, alongside newer botnets like Aisuru that build on Mirai's architecture.[source] Our own State of DDoS 2026 report found that IoT-based botnets (predominantly Mirai derivatives) account for 44% of all DDoS attack source IPs observed across the Flowtriq network.

CVE-2024-45163 does not eliminate the Mirai threat: new variants will eventually patch the flaw, and the underlying IoT infection vector remains unsolved. But it provides a meaningful disruption tool that shifts the economics of botnet operation. Every time a CNC server is crashed, the operator must restart it, reconnect bots, and resume operations. That friction matters.

More broadly, this discovery reflects our philosophy at Flowtriq: **understanding attacker infrastructure is as important as detecting attack traffic.** The better we understand how botnets operate, the more effectively we can detect, classify, and mitigate the attacks they produce.

Responsible Disclosure

CVE-2024-45163 was assigned by MITRE and published in the National Vulnerability Database on August 22, 2024. Given that Mirai is open-source malware operated by criminal actors, traditional responsible disclosure to a vendor does not apply. The vulnerability was disclosed publicly to maximize its defensive value.

CVSS Vector: `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H`

Translation: Network-exploitable, low complexity, no privileges required, no user interaction needed. High impact to integrity (CNC loses control of botnet) and availability (CNC crashes). No confidentiality impact.

Press Coverage

CVE-2024-45163 received coverage from major cybersecurity news outlets:

CYBERINSIDER

Researcher Discovers Kill-Switch for Mirai Botnet and Variants

August 26, 2024: Alex Lekander

SECURITY ONLINE

Hacking the Hacker: Researcher Found Critical Flaw in Mirai Botnet

August 25, 2024

CYBER SECURITY NEWS

Researchers Uncovered Remote DoS Exploit in Mirai Botnet

August 26, 2024: Eswar

HACKERDOSE

New Mirai Botnet Flaw That Could Cripple Cyber Attacks

August 26, 2024: Marco Rizal

Additional references:

- NIST National Vulnerability Database: CVE-2024-45163
- MITRE CVE Record: CVE-2024-45163
- GitHub Advisory Database: GHSA-cm9m-hp76-grcq
- Ogma: CVE-2024-45163 Mitigation Guide

Protect Your Infrastructure from Mirai

While CVE-2024-45163 disrupts the botnet's command channel, your infrastructure still needs to withstand the attacks that active botnets produce. Flowtriq detects Mirai-generated DDoS floods in under 1 second, classifies the attack vector with confidence scoring, and auto-mitigates with kernel-level firewall rules, BGP FlowSpec, and cloud scrubbing.

Detect and mitigate DDoS attacks in under 1 second.

Free 7-day trial. No credit card required. Installs in 2 commands.

START FREE TRIAL → SEE ALL FEATURES

Real-time DDoS detection, auto-mitigation, and instant alerting for infrastructure teams. Detect, mitigate, and communicate before your users notice.

FastNetMon Alternative

Migration Guide & Credit

LEGAL

Terms of Service

Privacy Policy

Data Processing

SLA

Security

Trust Center

Cookie Policy

SOC 2 / PCI / HIPAA

FREE TOOLS

Calculators

DDoS Downtime Cost Calculator

Bandwidth Cost Calculator

Incident Response Time Calculator

DDoS Risk Score Calculator

Packets Per Second Calculator

MTU / MSS Calculator

SLA Uptime Calculator

FastNetMon vs Flowtriq TCO Calculator

Scanners & Checkers

Is My Server Under Attack?

Open DNS Resolver Checker

NTP Amplification Scanner

Memcached Amplification Checker

DNS Propagation Checker

IP Threat Intelligence Lookup

Generators & References

Attack Vector Encyclopedia

Live DDoS Attack Map

Wireshark Filter Cheatsheet

Incident Response Plan Generator

iptables Rule Generator

nftables Rule Generator

Fail2Ban Config Generator

HAProxy DDoS Config

TCPDump Command Builder

BGP FlowSpec Rule Builder

PCAP Upload Analyzer

DDoS Attack Simulator

TCPDump/Wireshark Cheatsheet

Stay in the loop

Monthly attack postmortems, detection techniques, and engineering insights. No spam.

you@company.com SUBSCRIBE

Verifying...

Privacy • Help

All systems operational · View status →