Critical Authentication Bypass Vulnerability in GL.iNet GL-AXT1800 Router Firmware

Aleksa Zatezalo Follow 3 min read · Jan 8, 2026

Summary

A critical authentication bypass vulnerability has been discovered in the GL.iNet GL-AXT1800 (Slate AX) router firmware versions 4.2.0, 4.6.4, and 4.6.8. This flaw stems from the absence of rate limiting, CAPTCHA, or

account lockout mechanisms in the LuCI web interface's authentication endpoint. An unauthenticated attacker on the local network can perform unlimited brute-force attacks on admin credentials, potentially leading to full administrative access.This vulnerability can be chained with an authenticated command injection issue (detailed in a separate advisory) to achieve remote code execution (RCE) without initial authentication. Exploitation could result in complete device compromise, including unauthorized configuration changes, data exposure, and network infiltration.

Affected Products

- Vendor: GL.iNet
- Product: GL-AXT1800 (Slate AX)
- Affected Firmware Versions: 4.2.0, 4.6.4, 4.6.8
- Tested Platforms: Physical devices running the specified firmware
- Potentially Affected Models: Other GL.iNet routers using the LuCI web interface (unconfirmed further testing recommended)

Users should verify their firmware version through the router's web interface under System > Overview.

Vulnerability Description

The vulnerability affects the authentication endpoint at */cgi-bin/luci* in the LuCI web interface, which is based on OpenWrt. The endpoint processes POST requests containing *luci_username* and *luci_password* parameters without implementing any anti-brute-force measures. Successful logins

return an HTTP 302 redirect, while failures return HTTP 403, allowing attackers to automate attempts and identify valid credentials.Key issues:

No Rate Limiting: Unlimited requests can be sent without delay or restriction.

No Account Lockout: Accounts remain active regardless of failed attempts.

No CAPTCHA: No challenge-response mechanisms to prevent automation.

This is classified as CWE-307: Improper Restriction of Excessive Authentication Attempts.

Proof-of-Concept

An attacker can script repeated POST requests to brute-force passwords. A basic example using curl:

```
curl -d "luci_username=root&luci_password=<password_attempt>" http://<router_ip>
```

Monitor responses: HTTP 302 indicates success. Tools like Python scripts with wordlists can automate this, achieving high-speed attempts (e.g., thousands per minute) on a local network.Note: This PoC assumes local

network access. When chained with the command injection vulnerability, it enables full RCE.

Impact

Exploitation allows:

- Disclosure of admin credentials via brute-force.
- Unauthorized administrative access to the router.
- Modification of settings, such as Wi-Fi configurations, firewall rules, and DNS settings.
- Exposure of sensitive information, including connected device details and network traffic.
- Facilitation of further attacks, such as chaining with authenticated vulnerabilities for root-level RCE.

CVSS v3.1 Score: 6.5 (Medium)

- Vector: AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
- Breakdown: Adjacent network attack, low complexity, no privileges required, high confidentiality impact.

In a chained scenario with command injection, the overall impact escalates to high severity, enabling full system compromise.

Mitigation

- Update Firmware: Monitor for security patches from GL.iNet. As of this publication, no fix has been released. Check the vendor's security

advisories regularly.

- Use Strong, Unique Passwords: Replace default or weak passwords with complex ones (at least 12 characters, mixing types) to increase brute-force resistance.
- Disable WAN Access: Ensure the admin interface is not exposed to the internet restrict to LAN only.
- Implement Network Controls: Use VLANs or segmentation to limit local network access to the router's admin ports (80/443).
- Monitor Logs: Regularly review router logs for excessive failed login attempts.
- Vendor Fix: GL.iNet should add rate limiting (e.g., delay after failures), CAPTCHA, and temporary lockouts to the authentication endpoint.

If compromise is suspected, perform a factory reset and update to the latest firmware immediately.

Credits

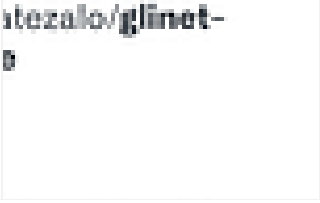
Researcher: Aleksa Zatezalo (Independent Security Researcher)

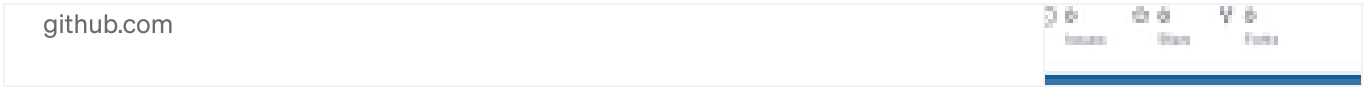
Tools Used: Custom Python exploit script (glinet_pwn.py), aiohttp, requests, passlib.

A full exploit chain can be found here:

GitHub — AleksaZatezalo/glinet-1800-rce

Contribute to AleksaZatezalo/glinet-1800-rce development by creating an account on GitHub.





Contact: For questions or collaboration, reach out via zabumaphu@gmail.com or @ZatezaloAleksa on X.com.

This advisory is provided for informational purposes. Use the information responsibly and only for authorized testing. Unauthorized exploitation may violate laws such as the Computer Fraud and Abuse Act (CFAA).

References

- GL.iNet Official Website: https://www.gl-inet.com
- GL.iNet Security Advisories: https://www.gl-inet.com/security/ (Note: Page was inaccessible at time of writing may be under maintenance)
- CWE-307: Improper Restriction of Excessive Authentication Attempts: https://cwe.mitre.org/data/definitions/307.html
- Related Exploit Code (for educational purposes): Available on GitHub (repository details withheld until CVE assignment contact author for access)
- MITRE CVE Program: https://cve.mitre.org

Hacking Routers VPN Zero Day Vulnerability

Written by Aleksa Zatezalo

586 followers · 17 following

Follow

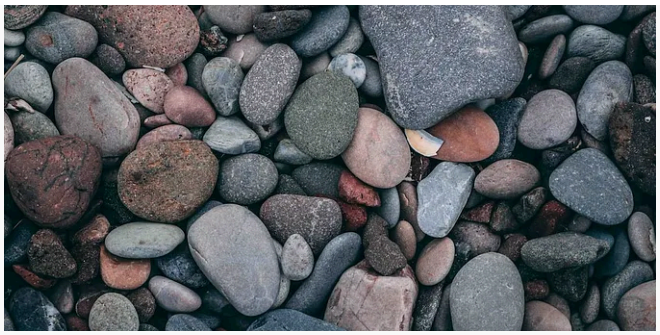
Interested in the intersection of Cloud, Cyber Security, and Artificial Intelligence.
Continually striving towards mastery of my domain. Forever an Apprentice.

No responses yet

Write a response

What are your thoughts?

More from Aleksa Zatezalo



In Offensive Security Library by Aleksa Zatezalo

OSCP Proving Grounds Walkthrough: Pebbels

Pebbles is a vulnerable machine on Offensive Securities Proving Grounds. It's catagorized...

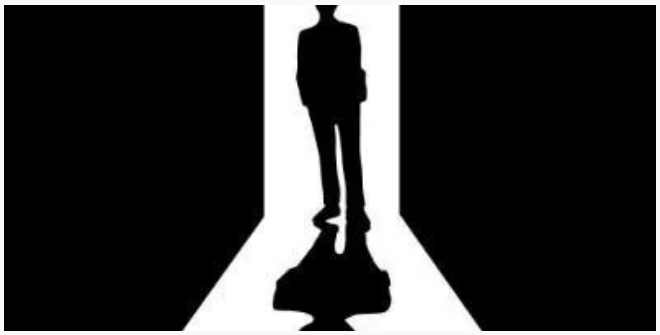
Aug 30, 2023

In InfoSec Write-ups by Aleksa Zatezalo

Extracting saved passwords in Chrome using python

Introduction

May 28, 2025

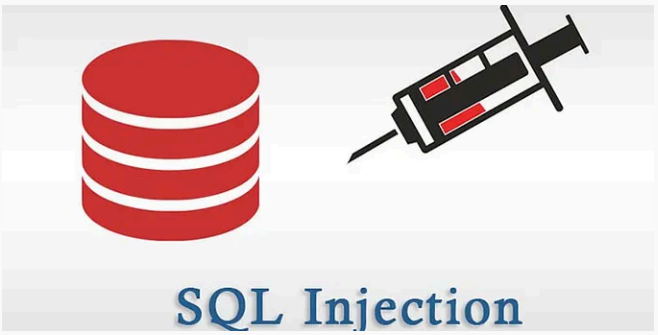


In Offensive Security Library by Aleksa Zatezalo

OSCP Proving Ground Walkthrough: Bratarina

Introduction

Aug 7, 2023



In InfoSec Write-ups by Aleksa Zatezalo

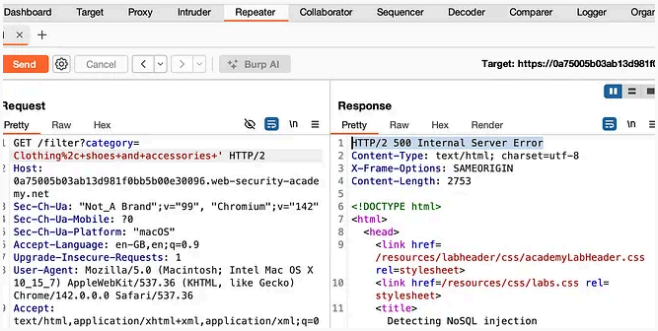
Finding my First SQL Injection On HackerOne

SQL injections have been a persistent aspect of web application security, maintaining thei...

Jan 19, 2025

See all from Aleksa Zatezalo

Recommended from Medium

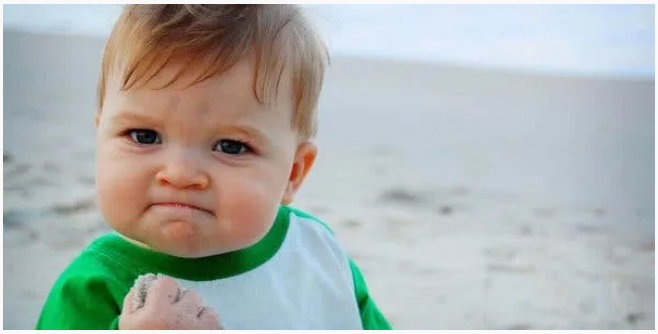


Kahhow

NoSQL injection

What is it, why it matters and noting steps to reproduce as documentation-of-learning

Nov 29, 2025

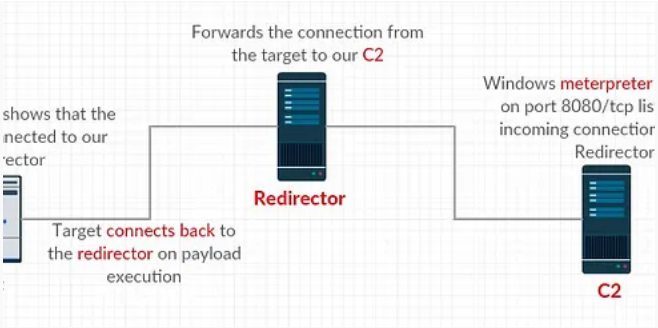


PARADOX

P1 Bug — Race Condition to Four Digit Bounty

Hey there, back again with another post! 😄

Jan 8



Youssef Said Thabet

Understanding Command & Control (C2)(C&C) — Part 1

What We will cover :

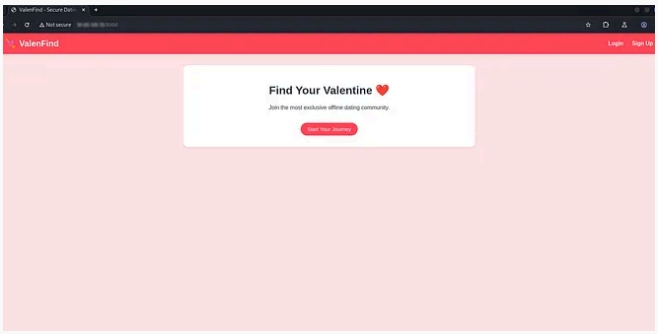
Feb 9

Aleksa Zatezalo

Authentication Bypass, Command Injection Vulnerability, and Race...

Authentication Bypass

Jan 8

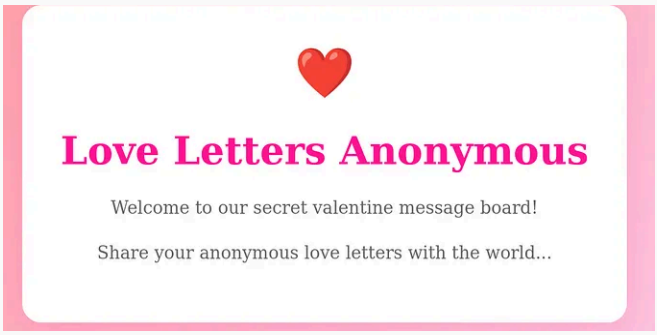


Sahand Babali

Valenfind Walkthrough (TryHackMe): Love at First Breach...

This challenge is from the Love at First Breach Valentine event on TryHackMe.

5d ago



Jatin Gahlot

Hidden Deep Into My Heart — LAFB CTF by TryHackMe

Hey Guys! 👋 This is a walkthrough of the task “Hidden Deep into My Heart” from the CTF...

4d ago

See more recommendations