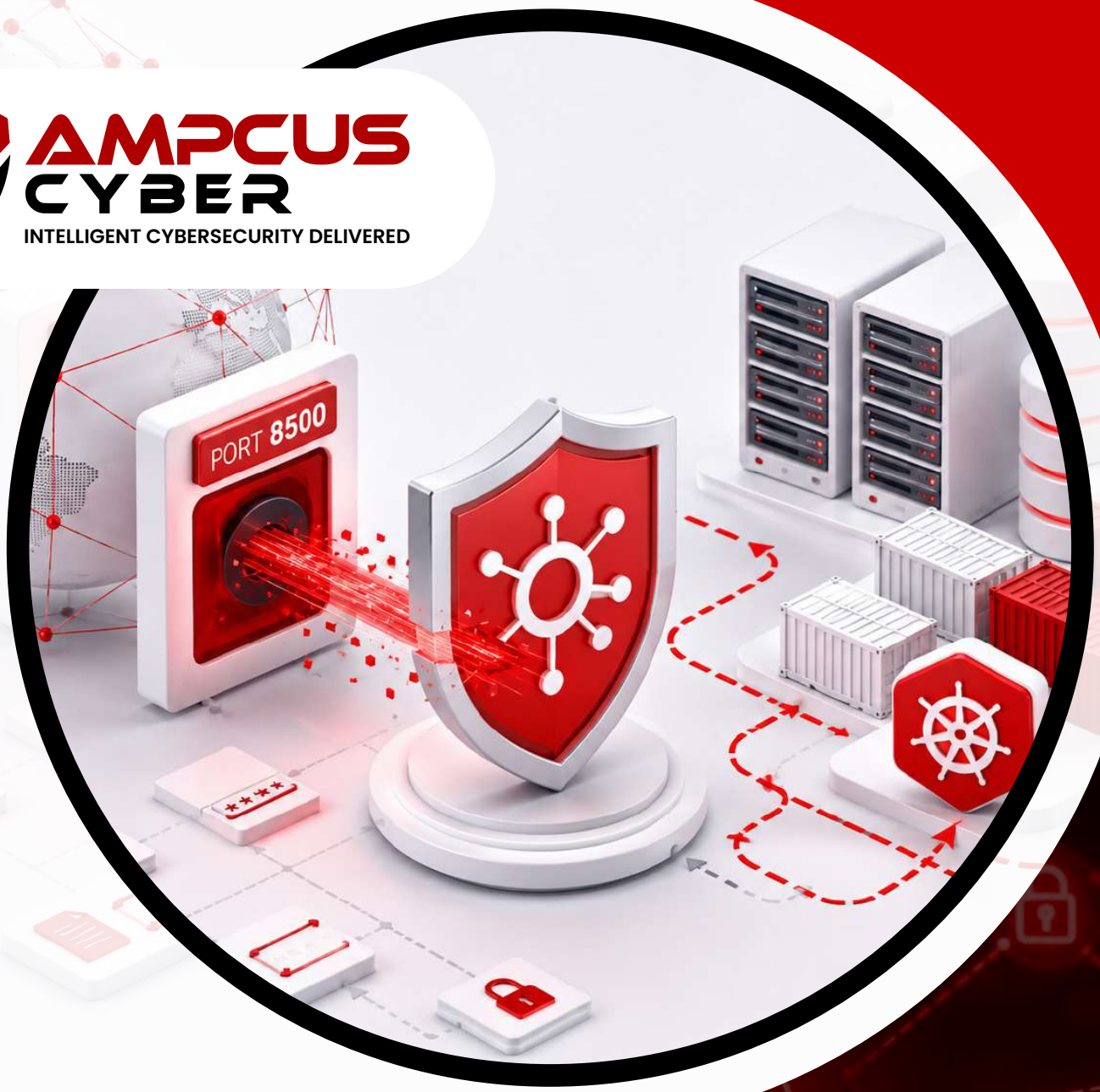
AMPCUS CYBER

INTELLIGENT CYBERSECURITY DELIVERED



From Port 8500 to Root: Exploiting an Exposed Consul Deployment

letsconnect@ampcuscyber.com

www.ampcuscyber.com

AMPCUS CYBER
INTELLIGENT CYBERSECURITY DELIVERED

Project Initiation and Scoping

Upon formal engagement, detailed scoping discussions with key stakeholders helped comprehensively outline the organization's external attack surface. This initial phase was critical for delineating the boundaries of the public-facing infrastructure and identifying key exposed assets. The core objective was to perform a comprehensive external penetration test against the internet-facing environment, searching for exploitable vulnerabilities that could compromise internal systems, data integrity, or service availability. Due to the sensitive nature of the engagement, the client's identity and specific infrastructure deployment models remain confidential.

Discovery Time	Public Port	Time to payload execution
Day 1	8500	~2 min

Immediate remediation actions
4

Environment Overview

The assessment focused on the organization's external-facing digital footprint:

Public-Facing Infrastructure:

- Comprised various internet-accessible services and applications.
- Utilized containerization and orchestration technologies, specifically leveraging
- Contained a critical misconfiguration that exposed internal orchestration services directly to the public internet on port 8500, entirely bypassing intended perimeter security controls.

Assessment Methodology and Execution

The active exploitation phase adopted a systematic approach from an external threat actor's perspective. On the very first day of the engagement, detailed reconnaissance and technical reviews quickly led to active exploitation.

During this initial assessment, a critical vulnerability was uncovered within the exposed service discovery architecture. The execution followed steps:

- **Reconnaissance and Port Scanning:** Initial external network scanning revealed that port 8500 was publicly accessible. Subsequent directory enumeration on this service uncovered an exposed endpoint at /v1/health/service/.

- **API Endpoint Analysis:** Further targeted enumeration pinpointed the HashiCorp Consul /v1/agent/service/register endpoint. Analysis confirmed this endpoint accepted unauthenticated PUT requests, granting unrestricted write access directly from the public internet.

- **Payload Development:** A specialized JSON payload was crafted to define a new service. This payload embedded a malicious system command within the service's "Health Check" script and included an Out-of-Band (OOB) link to capture and exfiltrate the execution response.

- **Exploitation and Execution:** The payload was uploaded via the unauthenticated PUT request. After a standard two-minute interval, the Consul agent automatically executed the health check script on the server side to verify the phantom service's status.

- **Container Compromise:** This successful injection enabled Remote Command Execution (RCE). To validate the impact, standard enumeration commands (including whoami, id, and cat /etc/shadow) were executed. The results confirmed execution with the privileges of the Consul process as root, granting complete access to the container.

- **Business Impact:** This unauthenticated access demonstrated a critical risk. Successful exploitation results in complete infrastructure compromise and the exposure of sensitive secrets. Furthermore, an attacker could leverage this rootlevel container access to perform lateral movement across the internal network, completely bypassing external perimeter controls.

AMPCUS CYBER
INTELLIGENT CYBERSECURITY DELIVERED

Remediation Support and Certification

Following the rapid identification of this critical RCE vulnerability, the organization was immediately notified to address the exposed Consul deployment. Remediation support included:

01 Immediate Network Restriction:

The primary and immediate fix involved blocking public access to port 8500 at the perimeter firewall level, successfully cutting off external access to the Consul API.

02 Configuration Review Guidance:

Guidance was provided on reviewing perimeter firewall rules to ensure internal orchestration ports are not inadvertently routed to the public internet.

03 Defense-in-Depth Recommendations:

Implementation of HashiCorp Consul Access Control Lists (ACLs) and the disabling of local script checks (enable_script_checks = false) were strongly advised to mitigate internal lateral movement risks.

04 Validation Testing:

Follow-up external scanning was conducted to verify that port 8500 was successfully closed and the API endpoints were no longer reachable from the internet.

Conclusion

This assessment highlighted the severe risks associated with exposing internal orchestration and service discovery tools to the public internet. Identifying this critical misconfiguration on the first day of testing demonstrated how unauthenticated API access can swiftly lead to a total, root-level container compromise. Through close collaboration during the immediate remediation phase, the organization successfully secured its perimeter and hardened its architecture, ensuring the environment is now resilient against similar external attack vectors