iterasec

# Securing the Client's External Network

**Client:**
Global Software Engineering Company

**Industry:**
Software Engineering and Technology Consulting

**Company Size:**
1500+ employees

**Services Used:**
External Network Pentesting, Vulnerability Research, Remediation Support

## Client

A global provider of software engineering, technology consulting, and quality assurance services, renowned for delivering innovative and high-quality solutions. Operating across multiple industries, this company helps businesses transform their operations with cutting-edge technology. Their extensive portfolio includes custom software development, product design, data science, and digital transformation services for clients worldwide.

## Background

As the company's operations expanded, so did the complexity of their external network environment. They maintained a range of public-facing services, including VPN servers, collaborative platforms like Jira and Confluence, and various websites accessible outside the company's perimeter. Recognizing the increasing threat landscape and the critical importance of safeguarding sensitive data, they sought to strengthen their cybersecurity posture, particularly concerning their demilitarized zones (DMZ) and external services. Additionally, annual compliance and certification standards mandated a thorough yearly assessment of these external-facing services, making robust security measures a top priority.

## The Challenge

The company engaged Iterasec to achieve several key objectives:

- **Comprehensive External Penetration Testing:**
  Conduct thorough security assessments of their external network infrastructure to identify vulnerabilities that could be exploited by malicious actors.
- **Critical Vulnerability Identification and Remediation:**
  Detect high-risk security flaws, especially those that could grant unauthorized access to internal systems or sensitive data.
- **Continuous Security Enhancement:**
  Provide iterative testing and validation to ensure that remediation efforts are effective and that security measures evolve with emerging threats.

## The Solution

Iterasec deployed a team of seasoned security professionals to execute a multi-phased penetration testing and security enhancement program.

### External Network Penetration Testing

- **Scope Definition:**
  Identified all external assets, including VPN endpoints, web applications, and public services like Jira, Confluence, and various company websites.
- **Exploitation of Critical Vulnerabilities:**
  Focused on exploiting vulnerabilities that could lead to significant security breaches, including unauthorized access to internal networks.
- **Vulnerability Scanning and Exploitation:**
  Utilized advanced tools and manual techniques to scan for vulnerabilities such as outdated software versions, misconfigurations, and exposed services.

### Discovery of Critical GLPI Vulnerability

During the assessment, we identified a critical vulnerability in the company's deployment of GLPI, an open-source IT asset management and service desk system. The vulnerability allowed us to:

- **Bypass Authentication:**
  Exploit an authentication bypass flaw to gain unauthorized access to the GLPI system.
- **Remote Access to Workstations:**
  Utilize GLPI's FusionInventory plugin to remotely access and control any workstation within the company network without administrative credentials.
- **Potential for Full Compromise:**
  Highlight the risk where an attacker could deploy backdoors or ransomware across the company's infrastructure using GLPI's software deployment functionalities.

### In-depth Vulnerability Research

- **Source Code Analysis:**
  Performed a comprehensive review of GLPI's publicly available source code to understand the root cause of the vulnerability.
- **Discovery of New CVE (CVE-2021-21327):**
  dentified a new vulnerability classified as CWE-470 (Use of Externally-Controlled Input to Select Classes or Code), which affected all GLPI instances up to version 9.5.3.
- **Responsible Disclosure:**
  Coordinated with the GLPI development team to report the vulnerability, leading to the issuance of CVE-2021-21327 and the release of a patched version (GLPI 9.5.4).

### Remediation Support

- **Immediate Mitigation:**
  Advised the company on temporary measures to secure their GLPI instance until a permanent fix was applied.
- **Patch Implementation:**
  Assisted in updating GLPI to the latest secure version and reconfiguring settings to enhance security.
- **System Hardening:**
  Provided recommendations on securing other external services by updating software, fixing misconfigurations, and enhancing monitoring.

### Iterative Testing and Validation

- **Follow-up Assessments:**
  Conducted additional penetration tests to verify the effectiveness of remediation efforts.
- **Continuous Monitoring:**
  Established protocols for regular security assessments to proactively identify and address new vulnerabilities.

## The Outcome

Our engagement led to substantial improvements in the company's security posture:

- **Elimination of Critical Vulnerabilities:**
  Successfully identified and helped remediate severe security flaws that could have led to a complete system compromise.
- **Strengthened External Security:**
  Enhanced the security of all external-facing services, reducing the attack surface and mitigating the risk of unauthorized access.
- **Improved Operational Resilience:**
  By addressing vulnerabilities in systems like GLPI, the company avoided potential disruptions that could have impacted their operations and client services.
- **Contribution to the Wider Community:**
  The discovery and disclosure of CVE-2021-21327 not only protected our client but also improved security for other organizations using GLPI.

## Conclusion

Our collaboration with the company underscores Iterasec expertise in delivering advanced cybersecurity solutions tailored to complex technological environments. By conducting thorough penetration testing and engaging in deep vulnerability research, we were able to uncover and address critical security issues that standard assessments might have missed.

Our proactive approach and technical acumen enabled the company to:

- Maintain trust with their clients by safeguarding sensitive information.
- Enhance their security infrastructure without disrupting ongoing operations.
- Stay ahead of emerging threats through continuous security improvement.

This case demonstrates the importance of not only addressing known vulnerabilities but also actively seeking out unknown risks that could pose significant threats. Iterasec remains committed to partnering with organizations to protect their assets and support their mission-critical objectives.