SYNOPSYS®

Thick Client Testing

Customized to fit the unique needs of your thick client software

Overview

Because security testing efforts often focus on web and mobile applications, many thick client applications don't undergo rigorous analysis. However, these applications can contain serious security problems, including memory corruption vulnerabilities, injection vulnerabilities, cryptographic weaknesses, and client-side trust issues. Such vulnerabilities can lead to a complete compromise of systems where the thick client software is installed, unauthorized access to server-side information, and more.

Thick client applications involve both local and server-side processing and often use proprietary protocols for communication. They may also contain multiple client-side components running at different trust levels. Simple, automated vulnerability assessment scanning isn't enough. That's why we customize each of our thick client tests to the application.

An approach as unique as your software

Our thick client application assessments start with a risk-based analysis of both your thick client software and the server-side APIs it communicates with. The analysis identifies:

- High-risk areas in the system
- Assets
- Attackers
- Potential attack vectors

This information, combined with a list of your business risks, gives us a blueprint for testing your thick client software.

Risk-based approach with 5 tracks of analysis

1. Automated scan

We use a proprietary tool to find common issues in the thick client software. The tool also enumerates the thick client's network communication, interprocess communication, operating system interactions, and more for our experts to analyze.

2. Configuration analysis

Our experts analyze your thick client's configuration, identifying both default configuration problems and ways the application could be configured to bypass security controls. This analysis also ensures that your software uses security features provided by the platform that it runs on.

3. Network communication analysis

Many thick client attacks involve remote execution. When this is the case, we intercept and analyze network communication in depth and reverse engineer custom protocols when needed. We use a proprietary tool to intercept and modify traffic regardless of the protocol used. We also write plugins for custom protocols to decrypt and parse packets so that we can perform deep analysis.

4. Server analysis

Most thick clients access some server-side functionality, and the successful exploit of a vulnerability in server-side code can affect all thick clients or central data stores. We analyze the server software using various manual and automated tools during this phase.

5. Client analysis

We analyze the thick client software itself using a variety of tools. Depending on the specific software and attacks of concern. activities may include performing memory dumps, testing IPC channels that may permit privilege escalation, fuzzing file inputs, and in-depth reverse engineering.

Beyond security testing

Your thick client applications can contain your organization's intellectual property, so you want them to be resistant to reverse engineering and modification. Without expert analysis of binary hardening mechanisms, you won't know how easily an attacker can reverse engineer or modify your client-side code. We have experience testing obfuscated and hardened applications, breaking security controls such as white box cryptography, and more.

Key benefits

Experience. We've tested a wide variety of thick clients, from enterprise software to antivirus software and video games. We customize each assessment to focus on the risks that are most relevant for your software.

Comprehensiveness. Our blended manual and tool-based assessment approach includes a thorough analysis of results, detailed reporting, and actionable remediation guidance.

Flexibility. We recognize that every organization has a different risk profile and tolerance, so we tailor our approach to your needs and budget. We can adjust assessment scope and perform tests more efficiently with access to source code, design documentation, specifications, and so on.

Enablement. At the end of each assessment, we'll conduct a read-out call to walk you through positive findings and prioritized vulnerabilities based on their likelihood and impact if exploited. We'll offer mitigation recommendations for each vulnerability and help you develop an actionable remediation plan best suited to your needs. If we create any custom tools or scripts to test your thick client software, we'll provide these to you so that your testing teams can use them.

The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior.

For more information about the Synopsys Software Integrity Group, visit us online at www.synopsys.com/software.

Synopsys, Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com