Line-of-business applications: maintaining vigilance down to the last link

By Kossi DOH
Lead RedTeam departement CDA

The third category of vulnerabilities involves the line-of-business (LOB) applications used daily by staff members such as account management software, loan processing systems, and internal operational tools. An application can be hosted on a impeccably secured network and still remain vulnerable if it was not designed or configured with security in mind.

Unauthenticated Applications
Our assessments identified applications accessible on the network without requiring any authentication no username, no password. Anyone with basic network access can view, and in some cases modify, sensitive application data and core features. This is the digital equivalent of an office building leaving its front doors wide open with no reception desk or access control.

Publicly Accessible Activity Logs
System logs record all activities performed within an application, including user logins, operational transactions, and error reports. While essential for threat detection and incident response, logs often contain sensitive data. Misconfigured access controls allowed unauthorized users to view these logs without logging in, exposing internal details that should have remained confidential.

Directory Traversal: Breaking Out of the Intended Path
Certain file-handling applications fail to properly sanitize user-supplied file paths. An attacker can manipulate these requests to traverse the server's directory structure and access restricted system files including configuration files containing plaintext credentials. It is like requesting a specific document at a service desk and discovering that slight alterations to the request grant access to any file in the cabinet.

Key Takeaway
An organization’s security boundary does not stop at the perimeter firewall: every individual application must strictly verify who is accessing its resources and what they are allowed to do.

Recommendations

- **Enforce Authentication Everywhere:** Mandate robust authentication for every application handling sensitive data or functionality without exception.
- **Secure Application Logs:** Restrict access to log files exclusively to authorized administrative accounts and perform regular audits.
- **Implement Strict Input Sanitization:** Ensure server-side validation and sanitization for all user-supplied file paths to prevent directory traversal attacks.
- **Adopt Secure SDLC Practices:** Integrate security testing (SAST/DAST) directly into the software development lifecycle and procurement processes.