mFIN-CERT.tg

Cybersecurity in microfinance institutions in Togo: what our penetration tests reveal

By Kossi DOH

Lead RedTeam departement CDA

This section of our awareness series presents three new families of vulnerabilities identified by Cyber Defense Africa (CDA) during penetration testing engagements for microfinance institutions in Togo. The objective is to explain these risks in clear, accessible language without targeting any specific institution to enhance the sector's collective vigilance. The cases presented here share a common thread: they rely on well-documented vulnerabilities some known for years for which patches have long been available. Their successful exploitation serves as a reminder that a published vulnerability remains dangerous only as long as it goes unpatched, and actively poses a threat until remediated.

Known vulnerabilities that were never patched

The majority of major cyberattacks do not rely on secret or highly sophisticated techniques. Instead, they exploit publicly known and documented vulnerabilities for which a fix exists... but has simply not been applied. Our penetration tests highlighted two striking examples of this issue.

The Cisco Vulnerability That Creates Rogue Administrator Accounts (CVE-2023-20198)

This vulnerability affects the web management interface of certain Cisco network appliances (routers, switches). It enables an unauthenticated attacker without needing any username or password to create a new account with full administrative privileges on the device. Once this account is created, the attacker controls the device as if they were a legitimate administrator: they can view and modify network configurations, intercept traffic, or leverage the device as a pivot point into the rest of the information system. It is the digital equivalent of a visitor walking into a building's reception desk and issuing themselves a "Director" access badge completely unnoticed.

EternalBlue: A 2017 Vulnerability Still Active in 2024

EternalBlue is the code name given to a critical vulnerability in the Windows Server Message Block (SMB) file-sharing protocol. It gained global notoriety in 2017 during the WannaCry and NotPetya ransomware attacks, which crippled hospitals, manufacturing plants, and government agencies worldwide. Although Microsoft released a patch that same year, our assessments successfully exploited this exact vulnerability on several workstations and servers. This granted full control over those systems, allowing us to harvest user credentials up to those providing access to the institution's core central database. A single unpatched machine was all it took to compromise the entire information system.

Key Takeaway

A vulnerability that has been public and patchable for years remains a wide-open door as long as the fix has not been applied to every single affected system across the network.

Recommendations

- **Promptly update Cisco Systems:** Apply security updates immediately to affected Cisco devices and disable the web management interface if it is not strictly required.
- **Establish systematic patch management:** Implement a routine, centralized patch management process across the entire infrastructure covering both servers and workstations.
- **Disable SMBv1:** Completely remove and disable the obsolete SMBv1 protocol (the primary vector for EternalBlue) across all operating systems.
- **Maintain asset and vulnerability tracking:** Keep an accurate hardware/software inventory and continuously monitor for known vulnerabilities affecting those assets.