mFIN-CERT.tg

Legacy systems and factory defaults: inherited vulnerabilities

By Kossi DOH

Lead RedTeam departement CDA

The second category of vulnerabilities does not stem from a one-off misconfiguration, but from a long-term lack of maintenance: software left unpatched and equipment deployed without altering its original factory settings.

Unmaintained Software and Systems

Regardless of how well-designed software is, vulnerabilities inevitably surface over time. This is why vendors regularly release security patches. An obsolete system is one that no longer receives these updates or where available patches have simply not been applied. Our assessments identified several systems and modules in this exact state, presenting known vulnerabilities that allow **Remote Code Execution (RCE)**. Simply put, an attacker can execute arbitrary commands on the machine without needing credentials or physical access. This is the most critical class of vulnerability, as it can grant an attacker virtually complete control over the compromised host.

Factory Default Passwords Left Unchanged

Many network appliances including routers, firewalls, IP cameras, printers, and connected UPS units ship with a default administrator account and password. These credentials are standard across all units of the same model and are frequently published in the manufacturer's public documentation. When these default credentials are left unchanged during deployment, anyone who knows the device’s make and model (information often visible on a physical asset tag) can log in and alter its configuration. Our engagements uncovered this vulnerability across multiple devices the digital equivalent of installing a heavy armored door while leaving the manufacturer’s key under the doormat.

Key Takeaway

Any hardware or software that is deployed and subsequently forgotten inevitably becomes one of the easiest entry points for an attacker to exploit.

Recommendations

- **Maintain an accurate system inventory:** Keep an up-to-date catalog of all hardware and software, paired with a routine schedule for applying security patches.
- **Isolate end-of-life systems:** Decommission or network-segment legacy systems that are no longer supported by their vendor if immediate replacement is not feasible.
- **Enforce credential changes:** Systematically change all default credentials on new equipment prior to putting it into production.
- **Harden administrative access:** Restrict access to device management interfaces strictly to authorized personnel and designated management networks.