IOActive Security Advisory

Title	Lamassu Douro Bitcoin ATM – Multiple Vulnerabilities
Severity	High
Discovered by	Gabriel Gonzalez
Advisory Date	2024-03-05
CVEs	CVE-2024-0674, CVE-2024-0675, CVE-2024-0676

Affected Products

- Douro model Bitcoin ATM from Lamassu Industries AG
- The same software was found on the latest update TAR package, so these issues may also affect newer versions

Background

IOActive had the opportunity to access used Lamassu Bitcoin ATMs. Although the reviewed devices are no longer supported, it is possible that some are still in operation and that, as found reviewing current packages, some issues are still present in newer deployments.

Timeline

- 2022-11-02: IOActive discovers vulnerabilities

CVE-2024-0674: Privilege Escalation

Severity: High

Impact

An unprivileged user can gain root execution on the ATM, resulting in full access to the system and the ability to install malicious software on the device and access all of the peripherals.

Proof of Concept

In order to exploit the vulnerability, an unprivileged user just needs to create the file `/tmp/extract/package/updatescript.js` with an appropriate payload, then trigger the update process.

CVE-2024-0675: Kiosk Escape

Severity: High

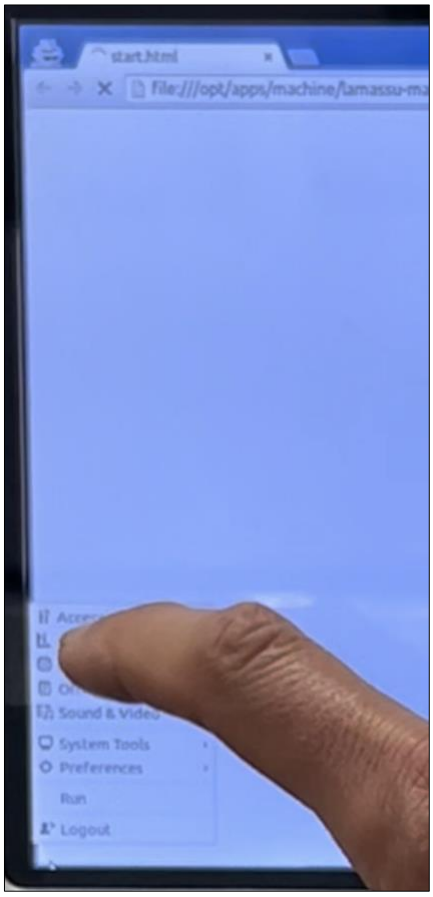
Impact

An attacker with physical access to an ATM can escape kiosk mode and access the underlying X Window interface. The attacker can then execute arbitrary commands as an unprivileged user.

Proof of Concept

During the booting process of the ATM interface, there are few seconds where the user can interact with the window manager installed on the Linux operating system.

As can be seen below, it is possible to access the menu, and from there open a terminal and other installed software.



CVE-2024-0676: Hardcoded Weak Password

Severity: High

Impact

An unprivileged user can elevate privileges to root via the `sudo` interface.

Technical Details

All analyzed devices shared the same weak (four-character) hardcoded password. By exploiting the above issues, IOActive acquired hashes from a compromised ATM. A dictionary-based attack cracked the password in a few minutes.

