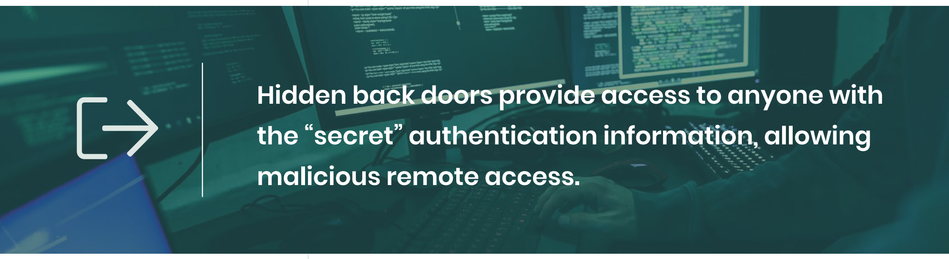
The Risk of Firmware Vulnerabilities

Unauthenticated Access

Web interface, telnet connections, or other access without authentication.

Allows unfettered access by arbitrary devices, making it effortless for attackers to gain access to the device interface and any controls provided by it.



Hidden back doors provide access to anyone with the "secret" authentication information, allowing malicious remote access.

Weak Authentication

Authentication mechanisms that are not robust and easily breached.

These range from simple password-based authentication mechanisms to systems based on weak cryptographic algorithms that can be broken by brute force attacks.

Hidden Back-Doors

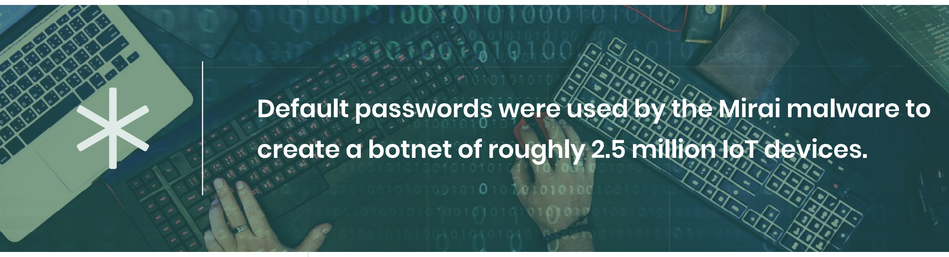
Hidden back-doors are inserted to allow developers access to systems after deployment.

While potentially helpful for customer support, the consequence when discovered by hackers are severe. And hackers are great at finding them.

Password Hashes Stored in Firmware

Hard-coded passwords that users are unable to change.

Many devices utilize hard-coded passwords, or default passwords that users rarely change, resulting in devices that are trivial to exploit.



Default passwords were used by the Mirai malware to create a botnet of roughly 2.5 million IoT devices.

Encryption Keys Stored in Firmware

Keys stored in firmware in an easily discoverable format.

Hackers use discovered keys to eavesdrop on communication, gain access to the device or even to create rogue devices that can perform malicious actions.

Buffer Overflows Vulnerabilities

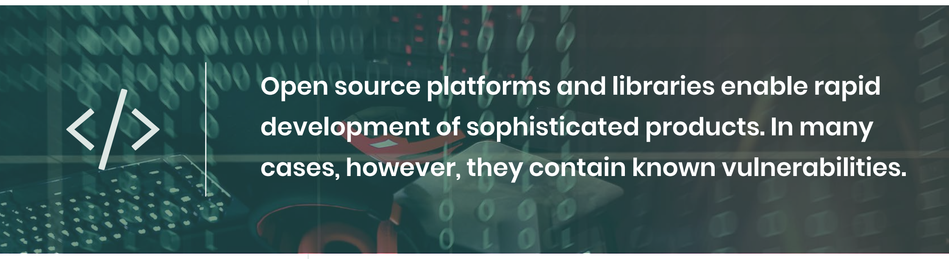
Use of insecure string handling functions may result in buffer overflows.

Buffer overflows can be exploited to create denial of service attacks and code injection attacks. Examples include using strcpy, strcat, etc. instead of the more secure strncpy, strncat counterparts.

Open Source Solutions w/Known Vulnerabilities

Automated hacking tools include exploits based on known vulnerabilities.

Often, simply updating to the latest version of the open source platform will address the vulnerability, yet many devices are released containing these vulnerabilities.



Open source platforms and libraries enable rapid development of sophisticated products. In many cases, however, they contain known vulnerabilities.

Debug Services in Production Systems

Debug systems in production devices provide hackers extra info and access.

Debug information gives developers internal systems knowledge of a device. When left in production, hackers gain that same inside knowledge and access.

CENTRIFUGE FIRMWARE SECURITY

refirmlabs.com

refirm labs

| info@refirmlabs.com | +1 (240) 389-2443 | Fulton, MD, USA 20759