A CVE-Driven Study Of OTA Firmware Vulnerabilities In IoT Devices

Student: Thohiru Omoloye
Supervisor: Paul Barry

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Introduction

The Internet of Things (IoT) sector is projected to exceed 18 billion connected devices globally. Over-the-Air (OTA) firmware updates represent one of the most operationally vital and most exploited attack surfaces in deployed IoT systems. When OTA channels are compromised, attackers can achieve persistent remote code execution, firmware modification, and long-term device takeover at scale.

Despite an expanding CVE record for IoT firmware vulnerabilities, the gap between vulnerability disclosure and actual patching in deployed devices remains poorly quantified. Existing literature focuses either on theoretical secure OTA protocols (e.g., IETF SUIT manifests for constrained devices) or broad firmware static analysis, leaving real-world exposure largely unmeasured.

This dissertation addresses that gap through a three-strand empirical design: CVE-based vulnerability analysis, Shodan-based real-world exposure mapping, and qualitative case studies combining to measure the disclosure-to-patch lag in live deployments.

Research Questions

RQ1. What are the most prevalent OTA firmware update vulnerabilities in IoT devices as documented in CVE records, and how are they distributed by CVSS severity and CWE category?

RQ2. To what extent do IoT devices with disclosed OTA firmware vulnerabilities remain publicly internet-exposed after the CVE disclosure date, as measurable via Shodan indexing?

RQ3. What patterns in vendor response, patch availability, and real-world update adoption characterise the OTA vulnerability lifecycle, as evidenced by selected case studies?

RQ4. How does CVSS severity correlate with the speed and completeness of firmware patching in deployed IoT devices?

Hypothesis

H1: OTA firmware vulnerabilities disproportionately present with CVSS scores in the High or Critical range (7.0+), reflecting systemic weaknesses in integrity verification and authentication mechanisms across IoT device categories.

H2: A statistically significant proportion of IoT devices with publicly disclosed OTA firmware CVEs will remain internet-exposed via Shodan for more than 6 months post-disclosure, indicating systematic failure in patch uptake across deployed device populations.

H3: Higher CVSS severity scores correlate with faster vendor patch release, but show no significant correlation with faster patch adoption in deployed devices, indicating vendor responsiveness does not drive user uptake.

Methodology

This study adopts an empirical, quantitative-dominant mixed-methods design structured around three evidence strands, shaped by supervisor feedback toward original data collection:

Strand 1: CVE Analysis

Systematic extraction of OTA-related CVEs from the NVD, filtered by CWE categories (CWE-494: Download Without Integrity Check; CWE-295: Improper Certificate Validation; CWE-306: Missing Authentication). CVSS v3.1 scores, attack vectors, and severity distributions are statistically analysed to characterise the threat landscape.

Strand 2: Shodan Exposure Mapping

Shodan API queries targeting device banners, firmware version strings, and product identifiers correlated to unpatched CVEs. This maps the live population of internet-exposed devices running vulnerable firmware, quantifying real-world exposure post-disclosure. Methodology follows the MDPI Electronics (vol.12/4815) template.

Strand 3: Qualitative Case Studies

3-5 in-depth case studies of high-profile OTA exploitation events provide contextual depth and triangulate quantitative findings, illuminating vendor response timelines and patching behaviours underlying the observed exposure data.