Critical Vulnerabilities in Campus Networks

Gabriel Minda

Abstract & Context

Universities in Latin America rely heavily on RUCKUS wireless infrastructures. However, budget constraints create critical security gaps. This study analyzes active exploits **(CVE-2023-25717)** enabling unauthenticated remote code execution.

We present a risk assessment and a cost-effective mitigation roadmap specifically designed for the regional context.

RuckusAPHardware

1. Objectives

- **Identify** critical attack vectors in RUCKUS ecosystems (AP & vSZ Controller).
- **Assess** the impact on Confidentiality, Integrity, and Availability (CIA).
- **Propose** a mitigation roadmap adapted to university budgets.

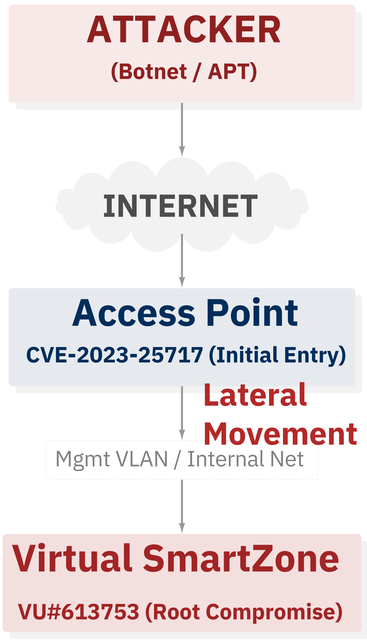
2. Critical Vulnerabilities Analysis

ID/Ref	Summary	CVSS
CVE-2023-25717	Unauth RCE in AP (HTTP Injection)	**9.8**
VU#613753	Multiple flaws (vSZ & RND)	**Crit.**
CVE-2025-44954	Root SSH via default keys	**10.0**

*Currently exploited by Andor yuBotfor DDoS attacks.

3. Attack Chain Visualization

Path from external threat to core infrastructure



4. Impact Analysis (CIA Triad)

Confidentiality

Exposure of RADIUS credentials, PII data, and user traffic monitoring.

Integrity

Firmware tampering and installation of persistent backdoors.

Availability

Campus-wide Wi-Fi blackouts or infrastructure used as DDoS zombies.

5. Mitigation Roadmap

Phase	Action	Items
Immediate	**Patch Firmware.** Isolate Mgmt VLANs. Rotate SSH keys. Restrict Admin IPs.	
Mid-Term	Deploy **Academic SOC** . NAC (Segmentation).	Implement
Long-Term	Governance alignment (ISO 27001). Vendor diversification.	Staff Training.

6. Key Performance Indicators (KPIs)

Metric Name	Target Goal
Secure Firmware Coverage	**100%**
Mean Time To Patch (Critical)	**< 7 Days**
Wireless Service Uptime	**> 99.5%**

7. Conclusions

Relying solely on vendor patches is insufficient. Universities must adopt a **Defense-in-Depth** approach combining **Network Segmentation**, **Active Monitoring**, and **Governance** to ensure academic continuity against modern threats.

8. References

F. Derenzin-Martínez, 593 Digital Publisher, 2024. SEGIB & CLAD, 2023. A. S. Tanenbaum et al., Computer Networks, 2011. NIST, "CVE-2023-25717," 2023. C. Lin, FortiGuard Labs, 2023. CERT/CC, "VU#613753," 2025. Claroty Team82, 2025. Ruckus Networks, Advisory 20250710. Ruckus Networks, UEES Case Study, 2025. Z. Zorz, Help Net Security, 2025.

Cybersecurity Fundamentals

Systems Engineering Student ✉ **gabominda1@gmail.com**