JIRBDAI Journal of Institutional Research, Big Data Analytics and Innovation

An Evaluation of Enterprise Router Management-Plane Security using Controlled Simulation

Bagu Jemimah Doosuur*[1], Oluwatobi N. Akande[2], Muhammed A. Suleiman[3]
1Department of Information Technology, Faculty of Computing, Nile University, Abuja, Nigeria
[2,3]Computer Science Department, Nile University of Nigeria, Abuja, Nigeria
*Corresponding Author: bobboaishaibrahim@gmail.com

ABSTRACT
Enterprise routers are often assumed secure just because they are used in business networks, but that assumption can be risky if management services are left open or poorly monitored, since unauthorized access might go unnoticed. This study examines enterprise router management plane security in a controlled GNS3 simulation. The objectives were to set up the simulation, test MikroTik RouterOS and Cisco IOS XE with controlled unauthorized access attempts, and evaluate performance using metrics such as service accessibility, authentication enforcement, logging visibility, mitigation, and system stability. A test network was created where an Ubuntu attacker node repeatedly tried to reach the management interfaces, and the systems recorded which services could be accessed, how authentication responded, what logs appeared, and the stability of the devices. After applying configuration changes to reduce exposure, the tests were repeated to review effectiveness. Both routers blocked unauthorized access, required valid credentials, and remained stable with no crashes or unexpected behavior. Logging behavior differed: MikroTik captured all access attempts, whereas Cisco's default setup didn't record failed web logins. After mitigation, certain management services became unreachable from the attacker node, reducing exposure. These results indicate that securing the management plane requires more than blocking logins. Administrator's team should disable unused services and ensure logging captures the attempts, while routers vendors should improve default logging. Proper configuration, ongoing monitoring, and observing system behavior are basis for maintaining enterprise router security and minimizing threats.

KEYWORDS: Enterprise Router Security, Management Plane, GNS3 Simulation, Logging Visibility, Access Control

I. INTRODUCTION
Enterprise routers sit at a central point in networks because they connect internal systems to external networks and support routing, access control, monitoring, and administrative management. As enterprise environments grow in scale and complexity, the security of these devices becomes more important because a weakness in router configuration or software can affect many connected systems at once. Router security is commonly viewed through the data plane, control plane, and management plane model, with the management plane covering the interfaces used by administrators to configure, monitor, and control the device. These interfaces may include commandline access, web-based management, and application interfaces such as REST services. Because management interfaces provide direct administrative control, they are attractive targets for unauthorized access attempts and other forms of abuse (Ceron et al., 2020; Ma et al., 2024; Qin et al., 2023).Previous studies like(Abu-Mahfouz et al., 2024; Chatzisofroniou & Kotzanikolaou, 2025; Freitas et al., 2024) have looked at different areas such as firmware vulnerabilities, IoT device exposure, and protocol weaknesses. Many of these studies focus on finding security flaws or detecting attacks in network traffic. It does not show how enterprise routers behave throughout management access attempts. Ceron et al. (2020),

Volume 2, Issue 1, 2026
https://doi.org/10.5281/zenodo.19733668

used honeypots to observe attacks on MikroTik devices. This method captures attack data, but it does not repeat testing under the same conditions. Other studies have used techniques like firmware analysis and vulnerability scanning to identify weaknesses in router systems. These approaches help to find possible security issues, but they do not show how routers enforce authentication, record events, or maintain stability at the access attempts. There is limited information on enterprise routers behavior when tested in a controlled and repeatable environment.

This work evaluates how enterprise routers deals with management plane access when unauthorized requests are made. We used a controlled simulation environment in GNS3, where the same tests can be repeated in the same conditions. The practical is carried out using MikroTik RouterOS and Cisco IOS XE in the same network setup to observe their behavior under identical test conditions. This aim to examine how management plane security act. The evaluation factors includes: whether management services are accessible, if authentication is used, access attempts are logged, and the two router's stability in the period of testing. It also examines how configuration changes affect these outcomes. To ensure consistency, each test is repeated 5 times. The same unauthorized request is sent from ubuntu attacker, and the responses from the routers are recorded. This makes it possible to observe behavior before and after configuration changes.

II. RELATED WORK

From 2020 to 2025 router security research concentrates on vulnerability discovery and attack detection. Ma et al. (2024) and Qin et al.(2023)examine embedded router firmware using static and binary analysis techniques to identify software weaknesses. While these studies expose the flaws, they do not assess management plane authentication behavior or runtime system response. Freitas et al. (2024)report largescale firmware exposure in national networks and identify 1,344 exploitable vulnerabilities. Their work focuses on vulnerability occurrence not logging visibility or response from the management plane. Ceron et al. (2020) use honeypots to analyze attacks targeting MikroTik router and confirm that exposed management services attract malicious activity. However, honeypot based observation does not evaluate router behavior under controlled and repeatable testing conditions. Pasupathi et al. (2025) and Hasan et al. (2023) apply machine learning techniques for distributed denial of service detection. These studies emphasize traffic classification and filtering not authentication enforcement, logging visibility, mitigation behavior, or system stability in enterprise routing platforms. Existing literatures therefore prioritizes vulnerability identification and traffic level attack detection. Limited research evaluates enterprise router management plane behavior using performance metrics under controlled simulation conditions. This gap motivates the present study. A summary of the related works is provided in Table 1.

III. METHODOLOGY

A. Evaluation Simulation Environment

A controlled and isolated GNS3 environment was used for the evaluation. The test network contained MikroTik RouterOS (CHR), Cisco CSR1000v running IOS XE, an Ubuntu Linux attacker node, and a shared subnet. This setup allowed repeated testing without exposing external systems or production networks. Figure 1 illustrates the network topology used in the study and shows how the attacker node interacts with both routers within a controlled environment.

Volume 2, Issue 1, 2026
https://doi.org/10.5281/zenodo.19733668

Table 1: Summary of Related studies

Authors (Year)	Methodology/Contributions	Results	Limitations
Chatzisofroniou & Kotzanikolaou. (2025)	Analyzes Wi-Fi Easy Connect for onboarding IoT; vulnerability and protocol tests on routers.	Design flaws allow unauthorized access/data interception; need stronger auth/firmware.	Wi-Fi protocol only; no broader evaluation or simulation.
Bonaventura et al. (2025)	Describes smart devices weakening home cybersecurity.	Insecure devices exploited, exposing networks/routers.	IoT focus, not direct router tests.
Pasupathi et al. (2025)	Proactive defense with packet marking, traffic analysis, ML for DDoS at router level.	Proactive defense with packet marking, traffic analysis, ML for DDoS at router level.	DDoS only
Kaushik et al.(2025)	Framework for reverse engineering/exploiting smart home firmware; maps to CVEs.	Identified high severity vulnerabilities; mitigation steps.	Firmware level; needs adaptation for vendor models in GNS3.
Kasama et al.(2025)	Large-scale analysis of default Wi-Fi SSID/passwords in 44 consumer routers.	30 models predictable; insecure defaults in field	Password focus
Batista et al. (2025)	Investigations on Eduroam security in Portuguese institutions; 802.1x/TLS configs.	Misconfigurations; inadequate guidance; recommendatios	Eduroam only; no CVE testing.
Park et al. (2025)	Lightweight secure FOTA for IoT; protocol design/security analysis.	Reduced attack exposure; integrity verification.	IoT-wide, not router specific.
Yue et al. (2025)	NPFTaint tool for exploitable vulnerabilities in Linux services via taint analysis.	Identified missed vulnerabilities; reduced false negatives.	Broad Linux; not tested on MikroTik/Cisco.
Ye et al.(2024)	Analyzed TLS in 40 home routers from 14 vendors.	Weak configs expose to MITM.	Consumer grade only.
Ma et al.(2024)	Static analysis of firmware web services with WFinder.	13 potential vulnerabilities across vendors.	Firmware only; no enterprise models.

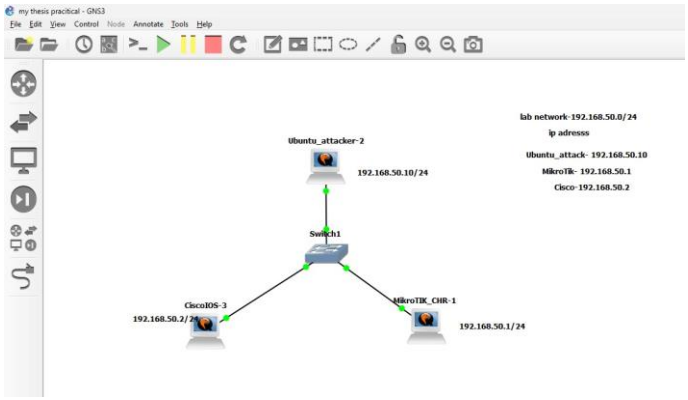

Figure 1 Network Topology in GNS3 Simulation for Enterprise Router Evaluation

Volume 2, Issue 1, 2026
https://doi.org/10.5281/zenodo.19733668

B. Evaluation Process Flow

The study followed a workflow made up of baseline setup, connectivity verification, controlled unauthorized access attempts, log inspection, mitigation, retesting, and comparative analysis. This framework was used to keep the procedure measurable and repeatable across both router platforms. Figure 2 illustrates the sequence of steps followed in the evaluation process, from initial setup to post-mitigation analysis, ensuring repeatability and controlled observation.

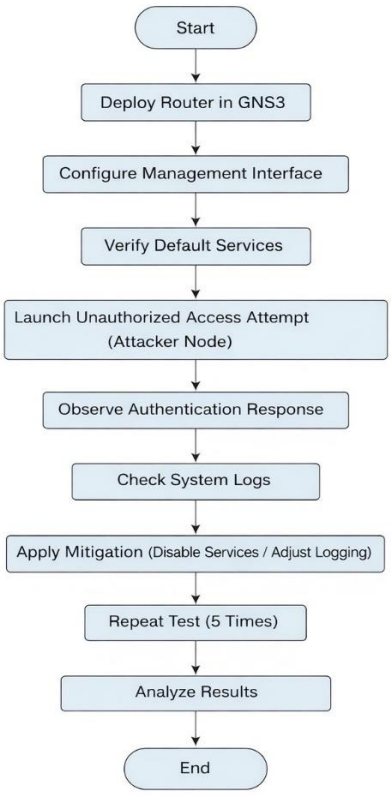

Figure 2. Management-plane Security Evaluation Process.

Figure 2 summarizes the sequence followed in the experiment. The process began with initial router configuration in GNS3 and verification that the required management services were active. Unauthorized access attempts were then launched from the Ubuntu node against the selected management interfaces. After each set of attempts, the routers were checked for authentication response, log visibility, and stability. Mitigation measures were then applied and the same access checks were repeated to observe changes in exposure. The same cycle was completed five times for each router so that variation across runs could be observed.

C. Evaluation Metrics

Each test was repeated five times to ensure consistency. The same set of access attempts was carried out in each run, and the results were recorded. To evaluate router behavior, five performance metrics were used. Each metric was calculated using ratios based on observed outcomes all along the testing.

(a). Service Accessibility Rate (%): This shows how often the management service responded to connection attempts. It is computed as follows:

$$Service\ Accessibility\ Rate\ = (Number\ of\ Successful\ Responses\ /\ Total\ Access\ Attempts) \times 100$$

Volume 2, Issue 1, 2026
https://doi.org/10.5281/zenodo.19733668

(b). Authentication Enforcement Rate (%): This indicates how consistently unauthorized access attempts were blocked. It is computed as follows:

$$\textbf{\textit{Authentication Enforcement Rate}} = \frac{Number\ of\ Rejected\ Unauthorized\ Attempts}{Total\ Unauthorized\ Attempts)}\ X\ 100$$

(c). Logging Visibility Rate (%): This reflects the extent to which access attempts were recorded in system logs. It is computed as follows:

$$Logging\ Visibility\ Rate\ = \frac{Number\ of\ Logged\ Events}{Total\ Access\ Attempts}\ X\ 100$$

(d). Mitigation Effectiveness Rate (%): This captures how much access was reduced after the configuration changes were applied. It is computed as follows:

$$Mitigation\ Effectiveness\ Rate = \frac{Number\ of\ Blocked\ Attempts\ After\ Mitigation}{Total\ Attempts}\ X\ 100$$

(e). **System Stability Rate (%):** This looks at system stability across test runs by checking for crashes, restarts, or performance issues. It is computed as follows:

$$System\ Stability\ Rate = \frac{Number\ of\ Stable\ Runs}{Total\ \ Runs}\ X\ 100$$

IV. Results and Discussion

The results were obtained from five repeated evaluations in the GNS3 environment. Most of the metrics produced constant outcomes across runs, since the behaviour of the routers did not change when undergoing tests. The only noticeable variation occurred in Cisco service accessibility, where one packet was lost in the first ICMP trial. For Cisco, the accessibility values across the five runs were 80%, 100%, 100%, 100%, and 100%. This gives an average of 96%, with a standard deviation of 8.94 percentage points. This small variation does not indicate a regular issue but a minor fluctuation observed at testing. This section presents the results and explains what they mean for management plane security.

(a). Management Service Accessibility: Management service accessibility disclose how exposed the management interfaces were before mitigation. For MikroTik RouterOS, accessibility checks succeeded before hardening, giving an aggregate accessibility rate of 100%. For Cisco IOS XE, 24 replies were received from 25 ICMP packets across five runs. This gives a total accessibility rate of 96%. The difference was caused by a single packet loss in the first trial not a steady issue. From a security perspective, both routers remained accessible to allow observation of management plane behaviour before mitigation.

(b). Authentication Enforcement: Both routers enforced authentication in all tested unauthorized access attempts. MikroTik returned HTTP 401 Unauthorized responses to REST API requests without valid credentials, while Cisco denied access to the web management interface and redirected the requester to authentication controls. This produced an authentication enforcement rate of 100% for both platforms within the tested conditions. This steady response was observed across all five test runs without variation. However, this value should be interpreted carefully. It takes into considerations the complete rejection of the specific requests used in this study, not absolute protection against every possible management plane attack.

(c). Logging Visibility: Logging visibility showed the clearest difference between the two routers. MikroTik RouterOS recorded the unauthorized management access attempts in time of the tests, resulting in a logging visibility rate of 100% under the active configuration. The logs included details such as source address, event timing, and login-related failures, which improves post event visibility and allows administrators to trace management plane activity effectively. In contrast, Cisco IOS XE did not generate persistent log entries for failed web authentication attempts under the default logging configuration used in this study, resulting in a logging visibility rate of 0%. This is a meaningful observation because authentication enforcement alone does not guarantee monitoring visibility. If unauthorized access attempts

https://doi.org/10.5281/zenodo.19733668

are rejected but not recorded, administrators may have limited evidence for incident analysis unless additional logging, debugging, or AAA related monitoring settings are enabled.

(d). Mitigation Effectiveness: After the initial tests, mitigation measures were applied by restricting or disabling exposed management services. When the Ubuntu node repeated the connection attempts, the targeted services were no longer reachable. This corresponds to a mitigation effectiveness rate of 100% for the post-mitigation checks carried out in this study. At the same time, this result should be interpreted within the scope of the evaluation, as it conveys the blocking of the tested access attempts after hardening instead of complete protection against possible management plane attack methods.

(e). System Stability: Throughout the evaluation, both routers continued to operate normally. There were no crashes, restarts, or noticeable performance issues during the repeated access attempts. This suggests that the type of activity generated in this study did not affect system operation.

(f). Overall Analysis: Taken together, the results show that management plane security is not just about blocking access. Authentication worked as expected on both devices, but visibility depended on configuration. MikroTik provided immediate insight into access attempts, while Cisco required additional setup to achieve the same level of monitoring. This illustrates the need to look beyond default settings when securing enterprise routers.

Table 2: Management Plane Security Evaluation Results

Metric	mikroTik RouterOS (%)	Ciscos IOS XE(%)
Service Acessibility Rate	100	96
Authentication Enforcement Rate	100	100
Logging visibility Rate	100	0
Mitigation effective Rate	100	100
System stability Rate	100	100

Table 2 summarizes the metric outcomes of the five repeated evaluations. The table shows that both platforms were consistent in authentication enforcement, mitigation response, and stability, while the main difference appeared in logging visibility. MikroTik provided both access rejection and event visibility, whereas Cisco provided access rejection without persistent default visibility for the tested web login events.

Volume 2, Issue 1, 2026
https://doi.org/10.5281/zenodo.19733668

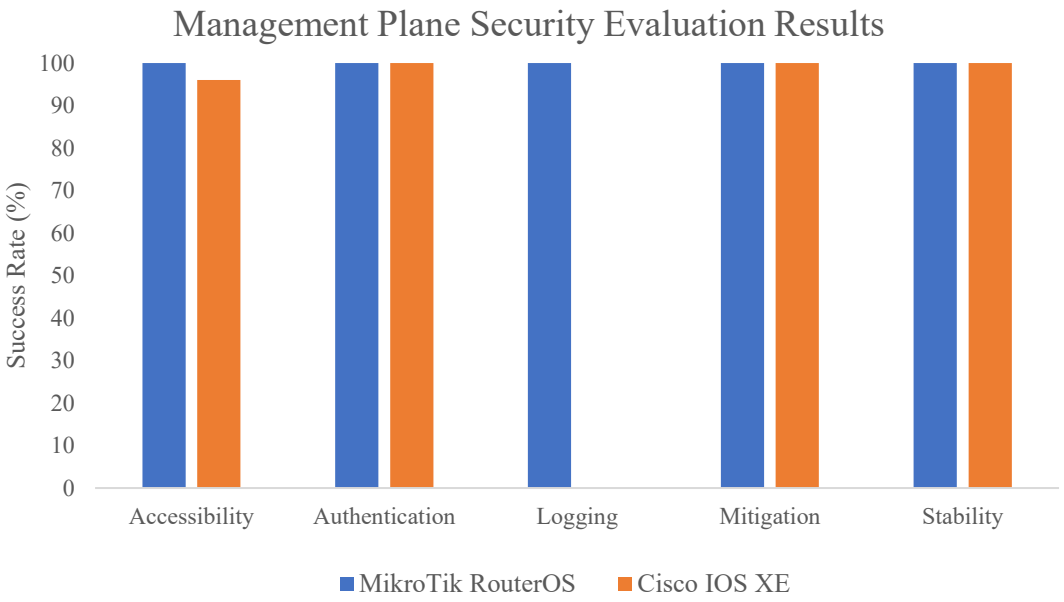

Figure 3. Management Plane Security Metrics Under Controlled Evaluation.

Figure 3 compares the five metrics across the two routers. The figure confirms that the strongest similarity between the platforms was authentication enforcement and operational stability, while the strongest difference was logging visibility. Because Cisco remained stable and rejected the requests but did not retain persistent log evidence for the tested web login failures, the figure helps show why management plane assessment should not stop at access denial alone.

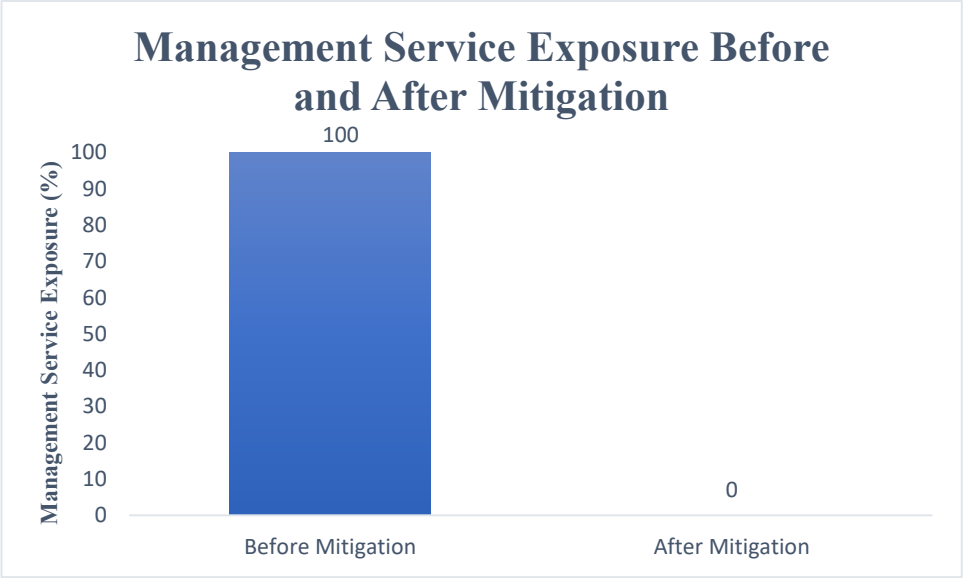

Figure 4. Effect of Management Service Mitigation

Figure 4 shows how management service exposure changed after mitigation was applied. Before the changes, the selected management services were reachable from the attacker node. After mitigation, the same checks no longer reached those interfaces. This represent the effect of reducing exposed services, especially when unnecessary management access is disabled or restricted. When considered alongside the logging results, it also suggests that limiting

Volume 2, Issue 1, 2026
https://doi.org/10.5281/zenodo.19733668

exposure and improving visibility work better when used together. Looking at the results, management plane security in this study depended on three main factors: consistent authentication enforcement, visibility of access attempts in the logs, and reduction of exposed services after mitigation Both MikroTik and Cisco rejected the tested unauthorized requests, but only MikroTik provided default log visibility for those events. This shows that similar access control outcomes do not always translate to the same level of support for monitoring and incident response.

V. CONCLUSION

This study evaluated management plane security on MikroTik RouterOS and Cisco IOS XE in a controlled GNS3 environment and found that both platforms rejected the unauthorized management access attempts used in the experiment and remained stable through the five runs. The main difference appeared in logging visibility: MikroTik recorded the tested access attempts, whereas Cisco IOS XE did not retain persistent log evidence for failed web authentication attempts under the default configuration examined. The study also showed that disabling or restricting unused management services reduced exposure in the lab environment. These findings suggest that effective management plane protection requires more than authentication alone; it also requires useful event visibility and reduction of unnecessary exposed services. Because the test covered two router platforms, one topology, and selected HTTP/HTTPS and REST API cases, the results should be interpreted within that limited scope. Future work can extend the design to additional vendors, multiple network conditions, and other management plane attack vectors such as SSH brute force, SNMP probing, and broader API attack setting.

REFERENCES

[1] Ceron, J. M., Scholten, C., Pras, A., & Santanna, J. (2020). MikroTik Devices Landscape, Realistic Honeypots, and Automated Attack Classification. *NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium*, 1–9. https://doi.org/10.1109/NOMS47738.2020.9110336

[2] Ma, X., Yan, C., Wang, Y., Wei, Q., & Wang, Y. (2024). A Vulnerability Scanning Method for Web Services in Embedded Firmware. *Applied Sciences (Switzerland)*, *14*(6). https://doi.org/10.3390/app14062373

[3] Qin, C., Peng, J., Liu, P., Zheng, Y., Cheng, K., Zhang, W., & Sun, L. (2023). UCRF: Static analyzing firmware to generate under-constrained seed for fuzzing SOHO router. *Computers & Security*, *128*, 103157. https://doi.org/10.1016/J.COSE.2023.103157

[4] Abu-Mahfouz, A., Alrabaee, S., Khasawneh, M., Gergely, M., & Choo, K. K. R. (2024). A Deep Learning Approach to Discover Router Firmware Vulnerabilities. *IEEE Transactions on Industrial Informatics*, *20*(1). https://doi.org/10.1109/TII.2023.3269774

[5] Chatzisofroniou, G., & Kotzanikolaou, P. (2025). Security analysis of the Wi-Fi Easy Connect. *International Journal of Information Security*, *24*(2), 74. https://doi.org/10.1007/s10207-025-00988-3

[6] Freitas, O., Taffarel, F., Santos, A., & Alves Pereira Junior, L. (2024). Uncovering Hidden Risks in IoT devices: A Post-Pandemic National Study of SOHO Wi-Fi Router Security. *Journal of Internet Services and Applications*, *15*, 485–495. https://doi.org/10.5753/jisa.2024.3834

[7] Pasupathi, S., Kumar, R., & Pavithra, L. K. (2025). Proactive DDoS detection: integrating packet marking, traffic analysis, and machine learning for enhanced network security. *Cluster Computing*, *28*(3), 210. https://doi.org/10.1007/s10586-024-04849-x

https://doi.org/10.5281/zenodo.19733668

[8] Hasan, A. H., Anbar, M., & Alamiedy, T. A. (2023). Deep learning approach for detecting router advertisement flooding-based DDoS attacks. *Journal of Ambient Intelligence and Humanized Computing*, *14*(6), 7281–7295. https://doi.org/10.1007/s12652-022-04437-0

[9] Bonaventura, D., Esposito, S., & Bella, G. (2025). A case of smart devices that compromise home cybersecurity. *Computers & Security*, *151*, 104286. https://doi.org/10.1016/J.COSE.2024.104286

[10] Kaushik, K., Bhardwaj, A., & Dahiya, S. (2025). Framework to analyze and exploit the smart home IoT firmware. *Measurement: Sensors*, *37*, 101406. https://doi.org/10.1016/J.MEASEN.2024.101406

[11] KASAMA, T., ISAWA, R., KAMINO, R., & HAGIWARA, Y. (2025). Unveiling the Security Risks in Default Wi-Fi Passwords of Consumer-grade Routers. *IEICE Transactions on Information and Systems*. https://doi.org/10.1587/transinf.2024ICP0007

[12] Batista, L. M., Gomes, H., & Almeida, J. R. (2025). Challenges and Solutions for Eduroam Network Security. *Procedia Computer Science*, *256*, 150–157. https://doi.org/10.1016/J.PROCS.2025.02.107

[13] Park, C.-Y., Lee, S.-J., & Lee, I.-G. (2025). Secure and Lightweight Firmware Over-the-Air Update Mechanism for Internet of Things. *Electronics*, *14*(8). https://doi.org/10.3390/electronics14081583

[14] Yue, S., Li, Q., Zhang, G., Li, X., Xu, B., & Tian, S. (2025). NPFTaint: Detecting highly exploitable vulnerabilities in Linux-based IoT firmware with network parsing functions. *Computers & Security*, 104679. https://doi.org/10.1016/J.COSE.2025.104679

[15] Ye, J., de Carné de Carnavalet, X., Zhao, L., Zhang, M., Wu, L., & Zhang, W. (2024). Exposed by Default: A Security Analysis of Home Router Default Settings and Beyond. *IEEE Internet of Things Journal*, *12*(2), 1182–1199. https://doi.org/10.1109/JIOT.2024.3502405