ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

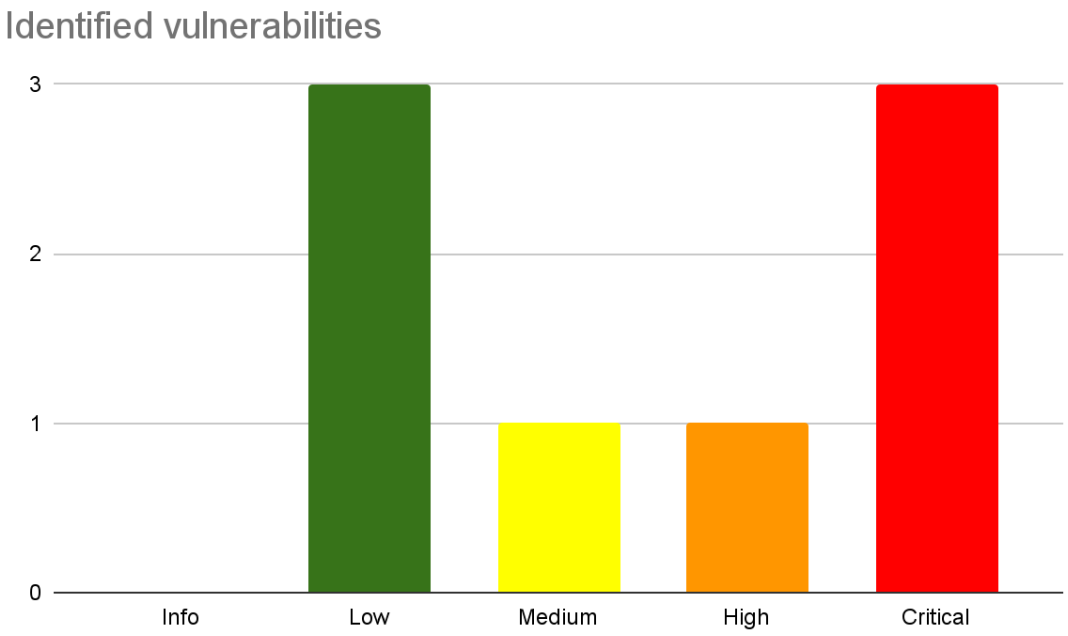
Πτυχιακή Εργασία

Τίτλος Πτυχιακής Εργασίας	Ανακάλυψη και εκμετάλλευση κρίσιμων κενών ασφαλείας σε δρομολογητές του εμπορίου Exploiting Consumer Routers with Unauthenticated Remote Code Execution
Ονοματεπώνυμο Φοιτητή	ΝΙΚΟΛΑΟΣ ΜΟΥΡΟΥΣΙΑΣ
Πατρώνυμο	ΔΗΜΗΤΡΙΟΣ
Αριθμός Μητρώου	Π/ 17076
Επιβλέπων	ΚΩΝΣΤΑΝΤΙΝΟΣ ΠΑΤΣΑΚΗΣ

Ημερομηνία Παράδοσης: Σεπτέμβριος 2024

Comprehensive Summary

In what follows, the research findings conducted in the scope of my dissertation at the Department of Informatics of the University of Piraeus are presented. The dissertation is focused on firmware security, which led to the study of Sercomm's VD4224BDT. The study discovered several vulnerabilities that, when combined, lead to a chained RCE exploit. The exploit allows an adversary to execute arbitrary code on Sercomm's VD4224BDT with root privileges. The following figure illustrates the severity of the vulnerabilities discovered in this research.



Given the context of the vulnerabilities and the business model of Sercomm, we have to stress that the vulnerabilities are ISP agnostic. Therefore, they are not part of a typical ISP customisation. As a result, it is **highly** probable that the vulnerabilities affect other ISPs that are using the same broadband router and other routers of the vendor. In this regard, while we report these findings for this firmware, other firmware must also be checked for these vulnerabilities.
The vendor has already confirmed these vulnerabilities and issued an appropriate patch. The most impactful vulnerabilities identified in this research have been assigned two CVE IDs: CVE-2024-55485 and CVE-2024-55486.

In addition to the identified vulnerabilities, a critical finding of this research pertains to firmware extraction methodologies. Our investigation demonstrates that a device's complete firmware can be retrieved by emulating an obsolete router and submitting a firmware update request to the Auto-Configuration Server (ACS). By exploiting insufficient authorization mechanisms inherent in the TR-069 protocol, an adversary could systematically obtain full firmware images for any router model managed by the ACS. This highlights a significant security risk, as unauthorized access to firmware enables reverse engineering, vulnerability discovery, and potential exploitation across entire device ecosystems.

Scope

The vulnerabilities described below assume unrestricted communication between the attacking device and the router. The attacking device could be a smartphone or computer using a web browser, assuming the user has clicked a malicious link. Additionally, the attack could be executed without user interaction (e.g., by clicking a link), provided the attacker is within the local network, such as a public Wi-Fi network in a café. These vulnerabilities specifically target the web configuration interface exposed internally within the network. The above is considered a light assumption, as it practically implies a typical user that is connected to the internet via the wired or wireless network interfaces that are provided by the router. Finally, in the case of a publicly exposed web interface, the attack can be launched remotely. In our latest Shodan search, approximately 200 users and businesses expose this interface to the public internet. Nevertheless, it is evident that the scale is far bigger since these devices are hardly exposed to the internet.

Identified vulnerabilities

Vulnerability	Command Injection
Risk	Critical
Detailed Description	The sanitisation checks performed on the input of diagnostic functions are insufficient and allow an adversary to inject arbitrary commands.
Impact	An adversary can execute arbitrary commands on the device with root permissions.
Recommendation	Sanitise the input that is used as input to system commands. The use of specialised libraries is highly recommended.
System/endpoint	/data/data.cgi
Reference	https://cwe.mitre.org/data/definitions/78.html

Vulnerability	Command Injection
Risk	Critical
Detailed Description	The configuration interface of internet services allows an adversary to inject arbitrary commands on multiple input fields.
Impact	An adversary can execute arbitrary commands on the device with root permissions.
Recommendation	Sanitise the input that is used as input to system commands. The use

	of specialised libraries is highly recommended.
System/endpoint	/data/data.cgi
Reference	https://cwe.mitre.org/data/definitions/78.html

Vulnerability	Authentication bypass
Risk	High
Detailed Description	The check to authenticate a user contains a logical flaw. An adversary can bypass the authentication mechanism by sending a specially crafted request.
Impact	An adversary can authenticate as an administrator without providing the necessary credentials.
Recommendation	Reimplementation of the authentication functionality is required. It is strongly suggested to incorporate standard Linux authentication mechanisms.
System/endpoint	The bug is triggered on any page that checks for a valid session.
Reference	https://cwe.mitre.org/data/definitions/288.html

Vulnerability	IP validation bypass
Risk	Medium
Detailed Description	The checks to determine that an actual IP has been provided can be bypassed due to the usage of inet_addr.
Impact	The improper checks on the input of inet_addr allow the adversary to submit further data that can be used to exploit other vulnerabilities.
Recommendation	Improve the input sanitisation mechanism for inet_addr. Consider the use of a dedicated library.
System/endpoint	Any functions that accept a user-supplied IP as input.
Reference	https://cwe.mitre.org/data/definitions/291.html

Vulnerability	Unauthenticated logout
Risk	Low
Detailed Description	An unauthorised request can log out a user.

Impact	While theoretically, this is a minor bug, it can be further combined with other bugs, facilitating the exploitation of the device.
Recommendation	Check whether the POST request has been made from an authenticated user.
System/endpoint	/data/login.json
Reference	https://cwe.mitre.org/data/definitions/284.html

Vulnerability	Insufficient Host Header validation
Risk	Low
Detailed Description	The web server fails to validate the Host header in incoming HTTP requests.
Impact	The server is vulnerable, among others, to DNS rebinding attacks. In the latter case, the attacker tricks a web browser into changing the destination IP address from a public IP to the router's IP, issuing remote requests to the router.
Recommendation	Implement strong Host header validation by allowing only the router's IP in the Host header.
System/endpoint	Generic request handling.
Reference	https://cwe.mitre.org/data/definitions/644.html

Vulnerability	Missing Security Headers
Risk	Low
Detailed Description	The X-Frame-Options header is missing from some HTTP responses.
Impact	An adversary can manipulate some requests and launch an attack from the browser, bypassing browser protections.
Recommendation	Add the X-Frame-Options header to all HTTP responses, even in static files like JavaScript/CSS.
System/endpoint	Generic request handling.
Reference	https://cwe.mitre.org/data/definitions/693.html