HAWKTESTERS

AUGUST 2024

HARDCODED CREDENTIALS

CVE-2024-46238

PRESENTED BY

Table of Contents

Vulnerability Description

Presentation of CVE-2024-46328

Issue

Hawktesters identifies a vulnerability in the `VONETS VAP11G-300` router, on the `Http_handle` object that references the `settings` binary. The vulnerability allows identifying hardcoded and persistent credentials in the binary.

Mitigation

Especially in this product context the suggested solution is to use configuration files or environment variables that keep credentials encrypted for later use, avoid storing any hardcoded plaintext secrets in product binaries.

Versions Affected

The details can be seen in the following table.

Device Name	VAP11G_300
Hardware Version	VER6.0
Software Version	3.3.23.6.9 (Jun 9 2023 14:52:17)
Library Version	2022.11.23

Technical Description

Description

Vonets VAP11G-300 is a professional 300Mbps wifi bridge of small size that also performs the function of WiFi repeater. The new design is unique in the world and ensures long-lasting stability. It is based on IEEE 802.11n, IEEE 802.11b and IEEE 802.11g standards.

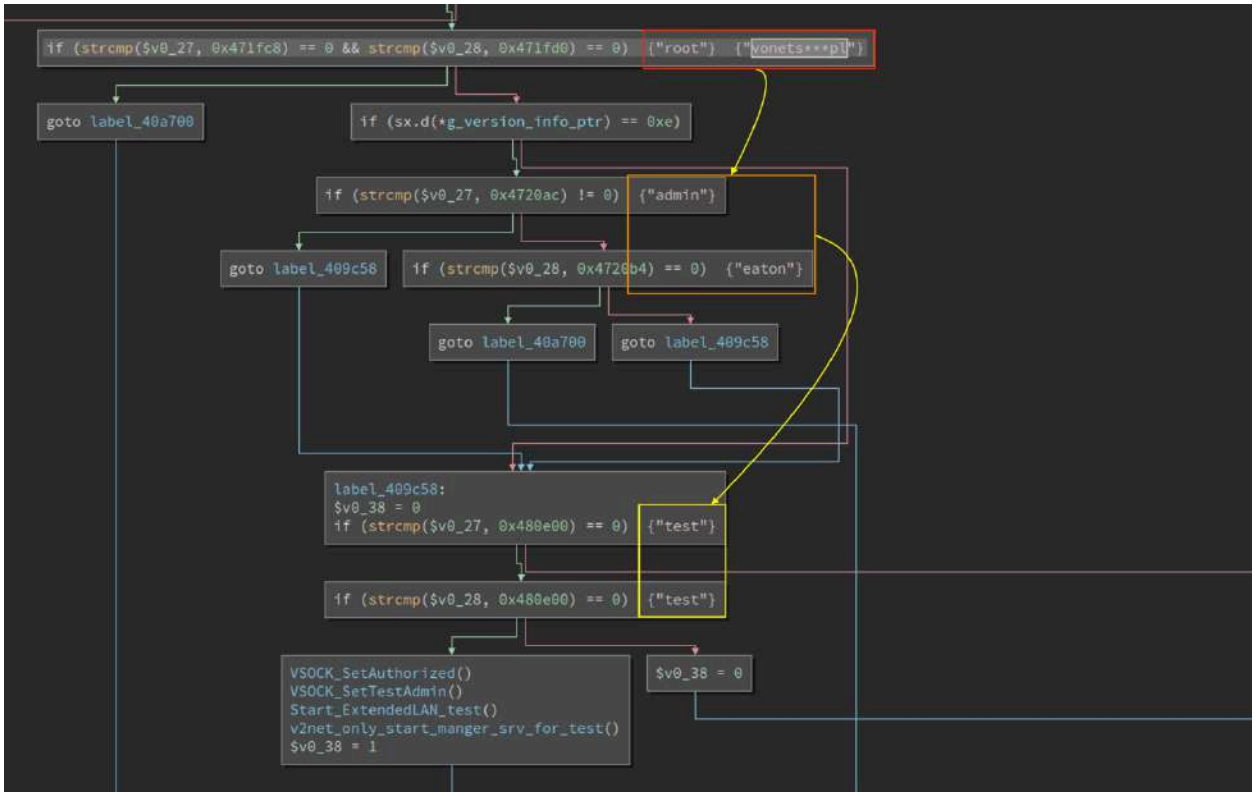
Issue(s)

Hawktesters discovers hardcoded credentials in the main settings binary, which allows an attacker to authenticate and take administrative control of the device.

Proof of Concept

User required: no

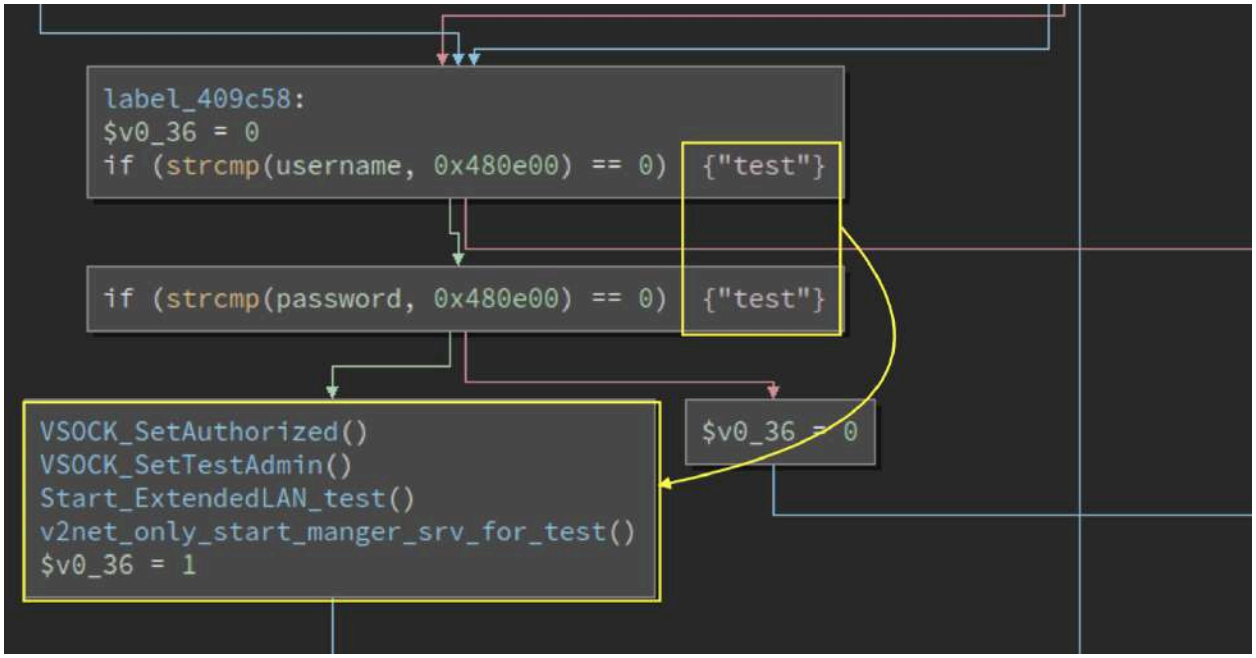
Compiling the main `settings` binary identifies the object named `Http_handle` which has associated authentication credentials hardcoded in the binary, these provide different access to the device, especially super-administrative.



The summary of credentials are as follows:

- `root:vonets***pl`
- `test:test`
- `admin:eaton`

In the following image you can see that the test:test credentials have a higher level of administrative privileges than the others.



Finally, by performing an HTTP request to the device's portal login you can check the functionality of the credentials.

Conclusions

Finally with the identified credentials, which are permanent in the binary despite factory resets, they can be used by an attacker to gain administrative privileges over the device without any restrictions.