

Scan Report

August 7, 2024

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone “Coordinated Universal Time”, which is abbreviated “UTC”. The task was “Immediate scan of IP 192.168.1.1”. The scan started at Wed Aug 7 08:30:51 2024 UTC and ended at Wed Aug 7 09:30:42 2024 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1	Result Overview	2
2	Results per Host	2
2.1	192.168.1.1	2
2.1.1	Medium 80/tcp	2

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.1.1 gpon.net	0	1	0	0	0
Total: 1	0	1	0	0	0

Vendor security updates are not trusted.

Overrides are off. Even when a result has an override, this report uses the actual threat of the result.

Information on overrides is included in the report.

Notes are included in the report.

This report might not show details of all issues that were found.

Issues with the threat level “Log” are not shown.

Issues with the threat level “Debug” are not shown.

Issues with the threat level “False Positive” are not shown.

Only results with a minimum QoD of 70 are shown.

This report contains result 1 of the 1 results selected by the filtering above. Before filtering there were 30 results.

2 Results per Host

2.1 192.168.1.1

Host scan start Wed Aug 7 08:31:37 2024 UTC

Host scan end Wed Aug 7 09:30:35 2024 UTC

Service (Port)	Threat Level
80/tcp	Medium

2.1.1 Medium 80/tcp

Medium (CVSS: 4.8)

NVT: Cleartext Transmission of Sensitive Information via HTTP

Summary

The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Quality of Detection (QoD): 80%

... continues on next page ...

...continued from previous page...

Vulnerability Detection Result

The following input fields were identified (URL:input name):

`http://gpon.net/:Frm_Password`

Impact

An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

Solution:

Solution type: Workaround

Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

Affected Software/OS

Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

Vulnerability Detection Method

Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.

The script is currently checking the following:

- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'

Details: Cleartext Transmission of Sensitive Information via HTTP

OID:1.3.6.1.4.1.25623.1.0.108440

Version used: 2023-09-07T05:05:21Z

References

url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management

url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure

url: <https://cwe.mitre.org/data/definitions/319.html>

[\[return to 192.168.1.1 \]](#)