

# Scan Report

January 17, 2023

## 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 172.16.1.5 recon”. The scan started at Mon Jan 16 11:38:24 2023 UTC and ended at Mon Jan 16 11:51:49 2023 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

<b>1</b>	<b>Result Overview</b>	<b>2</b>
<b>2</b>	<b>Results per Host</b>	<b>2</b>
2.1	172.16.1.5 . . . . .	2
2.1.1	Medium 80/tcp . . . . .	2
2.1.2	Low general/icmp . . . . .	4
2.1.3	Low general/tcp . . . . .	5

## 1 Result Overview

Host	High	Medium	Low	Log	False Positive
<a href="#">172.16.1.5</a>	0	2	2	0	0
Total: 1	0	2	2	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 all 4 results selected by the filtering described above. Before filtering there were 72 results.

## 2 Results per Host

### 2.1 172.16.1.5

Host scan start Mon Jan 16 11:38:54 2023 UTC

Host scan end Mon Jan 16 11:51:46 2023 UTC

Service (Port)	Threat Level
<a href="#">80/tcp</a>	Medium
<a href="#">general/icmp</a>	Low
<a href="#">general/tcp</a>	Low

#### 2.1.1 Medium 80/tcp

Medium (CVSS: 5.8)

NVT: WordPress User IDs and User Names Disclosure

##### Summary

WordPress platforms use a parameter called ‘author’. This parameter accepts integer values and represents the ‘User ID’ of users in the web site. For example: <http://www.example.com/?author=1>

##### Vulnerability Detection Result

... continues on next page ...

...continued from previous page ...
The following user names were revealed in id range 1-25. Discovered username 'recon' with id '1'
<b>Impact</b> These problems trigger the following attack vectors: 1. The query response discloses whether the User ID is enabled. 2. The query response leaks (by redirection) the User Name corresponding with that User ID.
<b>Solution:</b> <b>Solution type:</b> WillNotFix No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.
<b>Vulnerability Insight</b> The problems found are: 1. User ID values are generated consecutively. 2. When a valid User ID is found, WordPress redirects to a web page with the name of the author.
<b>Vulnerability Detection Method</b> Details: WordPress User IDs and User Names Disclosure OID:1.3.6.1.4.1.25623.1.0.103222 Version used: 2022-05-31T14:38:36Z
<b>References</b> url: <a href="http://www.talsoft.com.ar/index.php/research/security-advisories/wordpress-user-id-and-user-name-disclosure">http://www.talsoft.com.ar/index.php/research/security-advisories/wordpress-user-id-and-user-name-disclosure</a>

Medium (CVSS: 4.8) NVT: Cleartext Transmission of Sensitive Information via HTTP
<b>Summary</b> The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.
<b>Vulnerability Detection Result</b> The following input fields were identified (URL:input name): http://172.16.1.5/wp-login.php:pwd http://172.16.1.5/wp-login.php?redirect_to=http%3A%2F%2F172.16.1.5%2Fwp-admin%2F%26reauth=1:pwd
<b>Impact</b> ... continues on next page ...

...continued from previous page ...
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.
<b>Solution:</b> <b>Solution type:</b> 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.
<b>Affected Software/OS</b> Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.
<b>Vulnerability Detection Method</b> 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: 2020-08-24T15:18:35Z
<b>References</b> url: <a href="https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management">https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management</a> url: <a href="https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure">https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure</a> url: <a href="https://cwe.mitre.org/data/definitions/319.html">https://cwe.mitre.org/data/definitions/319.html</a>

[ [return to 172.16.1.5](#) ]

### 2.1.2 Low general/icmp

Low (CVSS: 2.1) NVT: ICMP Timestamp Reply Information Disclosure
<b>Summary</b> The remote host responded to an ICMP timestamp request.
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Solution:</b> <b>Solution type:</b> Mitigation
... continues on next page ...

...continued from previous page ...
<p>Various mitigations are possible:</p> <ul style="list-style-type: none"> <li>- Disable the support for ICMP timestamp on the remote host completely</li> <li>- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)</li> </ul>
<p><b>Vulnerability Insight</b></p> <p>The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp. This information could theoretically be used to exploit weak time-based random number generators in other services.</p>
<p><b>Vulnerability Detection Method</b></p> <p>Details: ICMP Timestamp Reply Information Disclosure  OID:1.3.6.1.4.1.25623.1.0.103190  Version used: 2022-11-18T10:11:40Z</p>
<p><b>References</b></p> <p>cve: CVE-1999-0524  url: <a href="http://www.ietf.org/rfc/rfc0792.txt">http://www.ietf.org/rfc/rfc0792.txt</a>  cert-bund: CB-K15/1514  cert-bund: CB-K14/0632  dfn-cert: DFN-CERT-2014-0658</p>

[\[ return to 172.16.1.5 \]](#)

### 2.1.3 Low general/tcp

<p>Low (CVSS: 2.6)  NVT: TCP timestamps</p>
<p><b>Summary</b></p> <p>The remote host implements TCP timestamps and therefore allows to compute the uptime.</p>
<p><b>Vulnerability Detection Result</b></p> <p>It was detected that the host implements RFC1323/RFC7323.  The following timestamps were retrieved with a delay of 1 seconds in-between:  Packet 1: 29465  Packet 2: 29734</p>
<p><b>Impact</b></p> <p>A side effect of this feature is that the uptime of the remote host can sometimes be computed.</p>
<p><b>Solution:</b>  <b>Solution type:</b> Mitigation</p>
... continues on next page ...

...continued from previous page ...
<p>To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.</p> <p>To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.</p> <p>See the references for more information.</p>
<b>Affected Software/OS</b> TCP implementations that implement RFC1323/RFC7323.
<b>Vulnerability Insight</b> The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.
<b>Vulnerability Detection Method</b> Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported. Details: TCP timestamps OID:1.3.6.1.4.1.25623.1.0.80091 Version used: 2020-08-24T08:40:10Z
<b>References</b> url: <a href="http://www.ietf.org/rfc/rfc1323.txt">http://www.ietf.org/rfc/rfc1323.txt</a> url: <a href="http://www.ietf.org/rfc/rfc7323.txt">http://www.ietf.org/rfc/rfc7323.txt</a> url: <a href="https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152">https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152</a>

[ [return to 172.16.1.5](#) ]