Agentless Vulnerability and Network Scanner Report

Scan Results

The following are the results of the agentless vulnerability and network scan.

Scanning IP: 10.10.19.106

Scanning IP: 10.10.19.106

Service: ssh, Version: 7.2p2 Ubuntu 4ubuntu2.4

Service: http, Version: 2.4.18

NVD: CVE-2016-1546 - The Apache HTTP Server 2.4.17 and 2.4.18, when mod_http2 is enabled, does not limit the number of simultaneous stream workers for a single HTTP/2 connection, which allows remote attackers to cause a denial of service (stream-processing outage) via modified flow-control windows. (Score: N/A)

NVD: CVE-2016-4979 - The Apache HTTP Server 2.4.18 through 2.4.20, when mod_http2 and mod_ssl are enabled, does not properly recognize the "SSLVerifyClient require" directive for HTTP/2 request authorization, which allows remote attackers to bypass intended access restrictions by leveraging the ability to send multiple requests over a single connection and aborting a renegotiation. (Score: N/A)

NVD: CVE-2018-1333 - By specially crafting HTTP/2 requests, workers would be allocated 60 seconds longer than necessary, leading to worker exhaustion and a denial of service. Fixed in Apache HTTP Server 2.4.34 (Affected 2.4.18-2.4.30,2.4.33). (Score: N/A)

NVD: CVE-2019-10082 - In Apache HTTP Server 2.4.18-2.4.39, using fuzzed network input, the http/2 session handling could be made to read memory after being freed, during connection shutdown. (Score: 9.1)

NVD: CVE-2023-2897 - The Brizy Page Builder plugin for WordPress is vulnerable to IP Address Spoofing in versions up to, and including, 2.4.18. This is due to an implicit trust of user-supplied IP

addresses in an 'X-Forwarded-For' HTTP header for the purpose of validating allowed IP addresses against a Maintenance Mode whitelist. Supplying a whitelisted IP address within the 'X-Forwarded-For' header allows maintenance mode to be bypassed and may result in the disclosure of potentially sensitive information or allow access to restricted functionality. (Score: 3.7)

Service: netbios-ssn, Version: 3.X - 4.X

Service: netbios-ssn, Version: 3.X - 4.X

Service: ajp13, Version:

Service: http, Version: 9.0.7

Vulnerability Overview

Vulnerability data in the form of pie chart: