

Denial-of-Service (CVE-2007-6750)

Domain: Justonweb.be

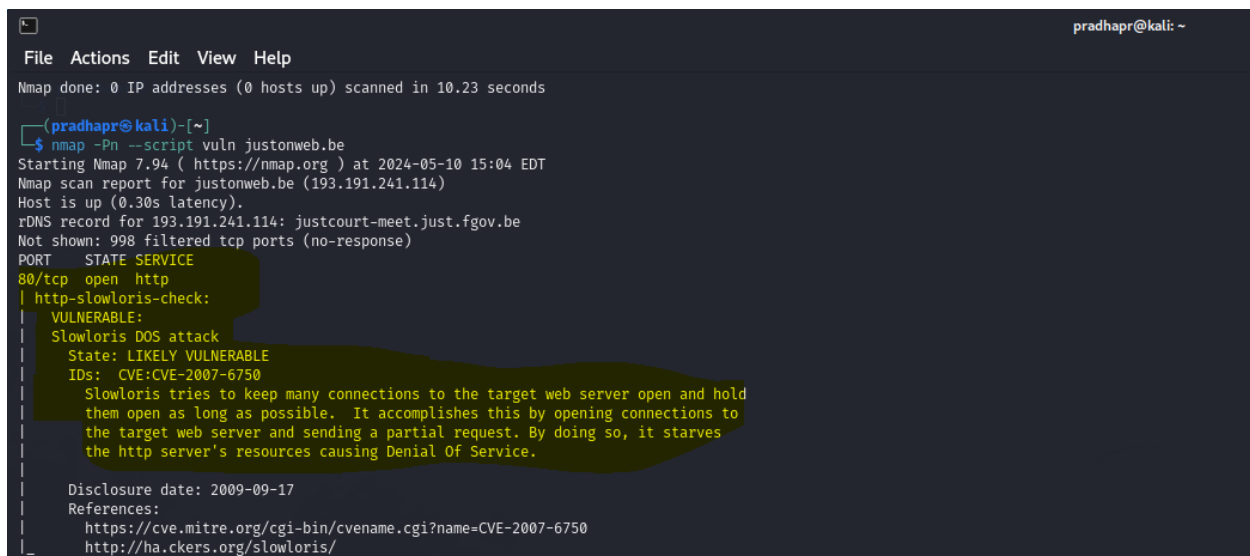
The vulnerability identified as CVE-2007-6750 affects Apache HTTP Server versions 1.x and 2.x. It enables remote attackers to execute a denial-of-service (DoS) attack on the server by exploiting a weakness in how the server handles partial HTTP requests. This vulnerability is particularly exploited through a technique known as Slowloris.

Vulnerability Description

Partial HTTP Requests: Attackers send partial HTTP requests to the server, keeping the connection open and waiting for more data.

Resource Exhaustion: The server's inability to handle these partial requests efficiently leads to resource exhaustion. Attackers can open multiple connections, consuming server resources without completing requests.

Proof of Concept



```
pradhapr@kali: ~  
File Actions Edit View Help  
Nmap done: 0 IP addresses (0 hosts up) scanned in 10.23 seconds  
  
(pradhapr@kali)-[~]  
$ nmap -Pn --script vuln justonweb.be  
Starting Nmap 7.94 ( https://nmap.org ) at 2024-05-10 15:04 EDT  
Nmap scan report for justonweb.be (193.191.241.114)  
Host is up (0.30s latency).  
rDNS record for 193.191.241.114: justcourt-meet.just.fgov.be  
Not shown: 998 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
80/tcp    open  http  
| http-slowloris-check:  
| VULNERABLE:  
| Slowloris DOS attack  
| State: LIKELY VULNERABLE  
| IDs: CVE:CVE-2007-6750  
| Slowloris tries to keep many connections to the target web server open and hold  
| them open as long as possible. It accomplishes this by opening connections to  
| the target web server and sending a partial request. By doing so, it starves  
| the http server's resources causing Denial Of Service.  
|  
| Disclosure date: 2009-09-17  
| References:  
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750  
| http://ha.ckers.org/slowloris/
```

Impact

The CVE-2007-6750 vulnerability allows attackers to launch DoS attacks against Apache HTTP Server, rendering it unavailable to legitimate users. This disrupts service availability and impacts user experience, potentially leading to financial losses and reputational damage.

Conclusion

Addressing the CVE-2007-6750 vulnerability is critical to mitigating the risk of DoS attacks against Apache HTTP Server. By implementing the proposed solutions and maintaining proactive security measures, organizations can enhance the resilience of their web servers and protect against exploitation by malicious actors.

```
(pradhapr@kali)-[~]
$ nmap -Pn -d --script vuln justonweb.be | grep "http-vuln-cve" | sort

/usr/bin/.. /share/nmap/scripts/http-vuln-cve2013-7091.nse:98: in function </usr/bin/.. /share/nmap/scripts/http-vuln-cve2013-7091.nse:61>
/usr/bin/.. /share/nmap/scripts/http-vuln-cve2014-3704.nse:219: in upValue 'do_sql_query'
/usr/bin/.. /share/nmap/scripts/http-vuln-cve2014-3704.nse:367: in function </usr/bin/.. /share/nmap/scripts/http-vuln-cve2014-3704.nse:337>
/usr/bin/.. /share/nmap/scripts/http-vuln-cve2014-3704.nse:219: bad argument #1 to 'match' (string expected, got nil)
NSE: Finished http-vuln-cve2009-3960 against justonweb.be (193.191.241.114:443).
NSE: Finished http-vuln-cve2009-3960 against justonweb.be (193.191.241.114:80).
NSE: Finished http-vuln-cve2010-0738 against justonweb.be (193.191.241.114:443).
NSE: Finished http-vuln-cve2010-0738 against justonweb.be (193.191.241.114:80).
NSE: Finished http-vuln-cve2010-2861 against justonweb.be (193.191.241.114:443).
NSE: Finished http-vuln-cve2010-2861 against justonweb.be (193.191.241.114:80).
NSE: Finished http-vuln-cve2011-3192 against justonweb.be (193.191.241.114:443).
NSE: Finished http-vuln-cve2011-3192 against justonweb.be (193.191.241.114:80).
NSE: Finished http-vuln-cve2011-3368 against justonweb.be (193.191.241.114:443).
NSE: Finished http-vuln-cve2011-3368 against justonweb.be (193.191.241.114:80).
NSE: Finished http-vuln-cve2012-1823 against justonweb.be (193.191.241.114:443).
NSE: Finished http-vuln-cve2012-1823 against justonweb.be (193.191.241.114:80).
NSE: Finished http-vuln-cve2013-0156 against justonweb.be (193.191.241.114:443).
NSE: Finished http-vuln-cve2013-0156 against justonweb.be (193.191.241.114:80).
NSE: Finished http-vuln-cve2013-6786 against justonweb.be (193.191.241.114:443).
NSE: Finished http-vuln-cve2013-6786 against justonweb.be (193.191.241.114:80).
NSE: Finished http-vuln-cve2013-7091 against justonweb.be (193.191.241.114:443).
NSE: Finished http-vuln-cve2014-2126 against justonweb.be (193.191.241.114:443).
NSE: Finished http-vuln-cve2014-2126 against justonweb.be (193.191.241.114:7443).
NSE: Finished http-vuln-cve2014-2127 against justonweb.be (193.191.241.114:443).
NSE: Finished http-vuln-cve2014-2127 against justonweb.be (193.191.241.114:7443).
NSE: Finished http-vuln-cve2014-2128 against justonweb.be (193.191.241.114:443).
NSE: Finished http-vuln-cve2014-2128 against justonweb.be (193.191.241.114:7443).
NSE: Finished http-vuln-cve2014-2129 against justonweb.be (193.191.241.114:443).
NSE: Finished http-vuln-cve2014-2129 against justonweb.be (193.191.241.114:7443).
NSE: Finished http-vuln-cve2014-3704 against justonweb.be (193.191.241.114:80).
NSE: Finished http-vuln-cve2014-8877 against justonweb.be (193.191.241.114:443).
NSE: Finished http-vuln-cve2014-8877 against justonweb.be (193.191.241.114:80).
NSE: Finished http-vuln-cve2015-1427 against justonweb.be (193.191.241.114:80).
NSE: Finished http-vuln-cve2015-1635 against justonweb.be (193.191.241.114:443).
NSE: Finished http-vuln-cve2015-1635 against justonweb.be (193.191.241.114:80).
NSE: Finished http-vuln-cve2017-1001000 against justonweb.be (193.191.241.114:443).
NSE: Finished http-vuln-cve2017-1001000 against justonweb.be (193.191.241.114:80).
NSE: Finished http-vuln-cve2017-5638 against justonweb.be (193.191.241.114:443).
NSE: Finished http-vuln-cve2017-5638 against justonweb.be (193.191.241.114:80).
NSE: Finished http-vuln-cve2017-8917 against justonweb.be (193.191.241.114:443).
NSE: Finished http-vuln-cve2017-8917 against justonweb.be (193.191.241.114:80).
NSE: Starting http-vuln-cve2009-3960 against justonweb.be (193.191.241.114:443).
NSE: Starting http-vuln-cve2009-3960 against justonweb.be (193.191.241.114:80).
NSE: Starting http-vuln-cve2010-0738 against justonweb.be (193.191.241.114:443).
```

```
NSE: Starting http-vuln-cve2010-0738 against justonweb.be (193.191.241.114:80).
NSE: Starting http-vuln-cve2010-2861 against justonweb.be (193.191.241.114:443).
NSE: Starting http-vuln-cve2010-2861 against justonweb.be (193.191.241.114:80).
NSE: Starting http-vuln-cve2011-3192 against justonweb.be (193.191.241.114:443).
NSE: Starting http-vuln-cve2011-3192 against justonweb.be (193.191.241.114:80).
NSE: Starting http-vuln-cve2011-3368 against justonweb.be (193.191.241.114:443).
NSE: Starting http-vuln-cve2011-3368 against justonweb.be (193.191.241.114:80).
NSE: Starting http-vuln-cve2012-1823 against justonweb.be (193.191.241.114:443).
NSE: Starting http-vuln-cve2012-1823 against justonweb.be (193.191.241.114:80).
NSE: Starting http-vuln-cve2013-0156 against justonweb.be (193.191.241.114:443).
NSE: Starting http-vuln-cve2013-0156 against justonweb.be (193.191.241.114:80).
NSE: Starting http-vuln-cve2013-6786 against justonweb.be (193.191.241.114:443).
NSE: Starting http-vuln-cve2013-6786 against justonweb.be (193.191.241.114:80).
NSE: Starting http-vuln-cve2013-7091 against justonweb.be (193.191.241.114:443).
NSE: Starting http-vuln-cve2013-7091 against justonweb.be (193.191.241.114:80).
NSE: Starting http-vuln-cve2014-2126 against justonweb.be (193.191.241.114:443).
NSE: Starting http-vuln-cve2014-2126 against justonweb.be (193.191.241.114:7443).
NSE: Starting http-vuln-cve2014-2127 against justonweb.be (193.191.241.114:443).
NSE: Starting http-vuln-cve2014-2127 against justonweb.be (193.191.241.114:7443).
NSE: Starting http-vuln-cve2014-2128 against justonweb.be (193.191.241.114:443).
NSE: Starting http-vuln-cve2014-2128 against justonweb.be (193.191.241.114:7443).
NSE: Starting http-vuln-cve2014-2129 against justonweb.be (193.191.241.114:443).
NSE: Starting http-vuln-cve2014-2129 against justonweb.be (193.191.241.114:7443).
NSE: Starting http-vuln-cve2014-3704 against justonweb.be (193.191.241.114:443).
NSE: Starting http-vuln-cve2014-3704 against justonweb.be (193.191.241.114:80).
NSE: Starting http-vuln-cve2014-8877 against justonweb.be (193.191.241.114:443).
NSE: Starting http-vuln-cve2014-8877 against justonweb.be (193.191.241.114:80).
NSE: Starting http-vuln-cve2015-1427 against justonweb.be (193.191.241.114:80).
NSE: Starting http-vuln-cve2015-1635 against justonweb.be (193.191.241.114:443).
NSE: Starting http-vuln-cve2015-1635 against justonweb.be (193.191.241.114:80).
NSE: Starting http-vuln-cve2017-1001000 against justonweb.be (193.191.241.114:443).
NSE: Starting http-vuln-cve2017-1001000 against justonweb.be (193.191.241.114:80).
NSE: Starting http-vuln-cve2017-5638 against justonweb.be (193.191.241.114:443).
NSE: Starting http-vuln-cve2017-5638 against justonweb.be (193.191.241.114:80).
NSE: Starting http-vuln-cve2017-8917 against justonweb.be (193.191.241.114:443).
NSE: Starting http-vuln-cve2017-8917 against justonweb.be (193.191.241.114:80).
NSE: [http-vuln-cve2009-3960 193.191.241.114:443] http.request socket error: The script encountered an error:
NSE: [http-vuln-cve2009-3960 193.191.241.114:443] http.request socket error: The script encountered an error:
```