Source Code Disclosure Vulnerability (CVE-2010-2333)

Domin: https://www.mercadopago.com.pe/

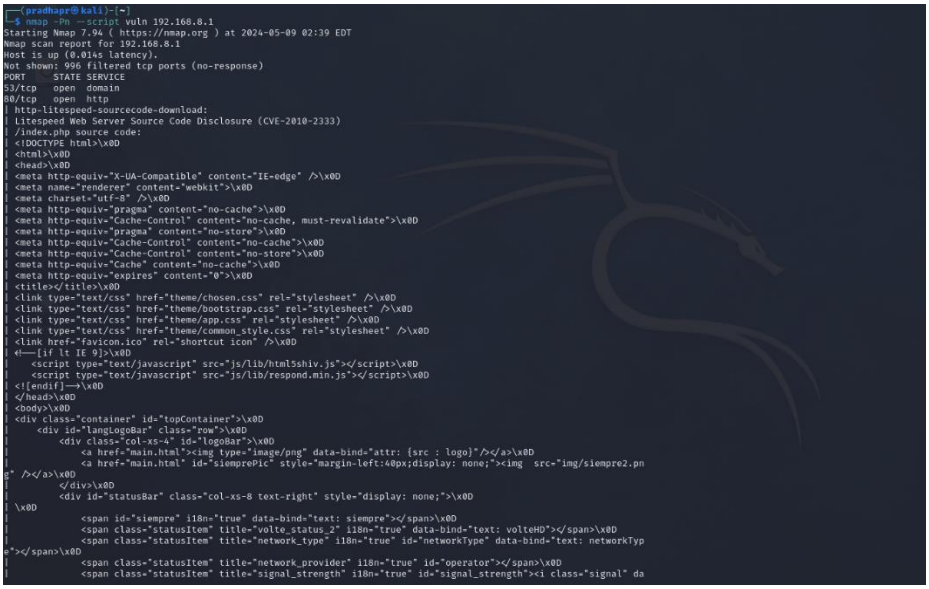
Description:

The Litespeed Web Server running on port 80/tcp has been identified to potentially expose source code through the /index.php file. This vulnerability, registered as CVE-2010-2333, could allow malicious actors to access sensitive information, including proprietary code or configurations.

Affected Components:

The /index.php source code within the Litespeed Web Server.

Proof of Concept:



```
┌──(pradhapr㉿kali)-[~]
└─$ nmap -Pn --script vuln 192.168.8.1
Starting Nmap 7.94 ( https://nmap.org ) at 2024-05-09 02:39 EDT
Nmap scan report for 192.168.8.1
Host is up (0.014s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
| http-litespeed-sourcecode-download:
| Litespeed Web Server Source Code Disclosure (CVE-2010-2333)
| /index.php source code:
| <!DOCTYPE html>\x0D
| <html>\x0D
| <head>\x0D
| <meta http-equiv="X-UA-Compatible" content="IE=edge" />\x0D
| <meta name="renderer" content="webkit">\x0D
| <meta charset="utf-8" />\x0D
| <meta http-equiv="pragma" content="no-cache">\x0D
| <meta http-equiv="Cache-Control" content="no-cache, must-revalidate">\x0D
| <meta http-equiv="pragma" content="no-store">\x0D
| <meta http-equiv="Cache-Control" content="no-cache">\x0D
| <meta http-equiv="Cache-Control" content="no-store">\x0D
| <meta http-equiv="Cache" content="no-cache">\x0D
| <meta http-equiv="expires" content="0">\x0D
| <title></title>\x0D
| <link type="text/css" href="theme/chosen.css" rel="stylesheet" />\x0D
| <link type="text/css" href="theme/bootstrap.css" rel="stylesheet" />\x0D
| <link type="text/css" href="theme/app.css" rel="stylesheet" />\x0D
| <link type="text/css" href="theme/common_style.css" rel="stylesheet" />\x0D
| <link href="favicon.ico" rel="shortcut icon" />\x0D
| <!--[if lt IE 9]>\x0D
|    <script type="text/javascript" src="js/lib/html5shiv.js"></script>\x0D
|    <script type="text/javascript" src="js/lib/respond.min.js"></script>\x0D
| <![endif]-->\x0D
| </head>\x0D
| <body>\x0D
| <div class="container" id="topContainer">\x0D
|     <div id="langLogoBar" class="row">\x0D
|         <div class="col-xs-4" id="logoBar">\x0D
|             <a href="main.html"><img type="image/png" data-bind="attr: {src : logo}"></a>\x0D
|             <a href="main.html" id="siemprePic" style="margin-left:40px;display: none;"><img  src="img/siempre2.pn
g" /></a>\x0D
|         </div>\x0D
|         <div id="statusBar" class="col-xs-8 text-right" style="display: none;">\x0D
| \x0D
|             <span id="siempre" i18n="true" data-bind="text: siempre"></span>\x0D
|             <span class="statusItem" title="volte_status_2" i18n="true" data-bind="text: volteHD"></span>\x0D
|             <span class="statusItem" title="network_type" i18n="true" id="networkType" data-bind="text: networkTyp
e"></span>\x0D
|             <span class="statusItem" title="network_provider" i18n="true" id="operator"></span>\x0D
|             <span class="statusItem" title="signal_strength" i18n="true" id="signal_strength"><i class="signal" da
```

```
File  Actions  Edit  View  Help
|             <span class="statusItem" title="network_provider" i18n="true" id="operator"></span>\x0D
|             <span class="statusItem" title="signal_strength" i18n="true" id="signal_strength"><i class="signal" da
ta-bind="attr:{'class': signalCssClass}"> </i></span>\x0D
|             <span class="statusItem" title="connection_status" i18n="true" id="connection_status"><i class="icon_c
onnection" data-bind="attr:{'class': connectionCssClass}"> </i></span>\x0D
|             <span class="statusItem" title="rj45_connection_status" i18n="true" id="rj45_connection_status" data-b
ind="visible: false"><i class="icon_connection" data-bind="attr:{'class': rj45ConnectionCssClass}"> </i></span>
\x0D
|             <span class="statusItem" title="sms_unread_count" i18n="true" id="sms_unread_count" data-bind="visible
: smsUnreadCount() > 0 || showSmsDeleteConfirm()" style="display: none; position: relative;">\x0D
|                 <a onclick="return gotoSmsList();" href="javascript: void(0)">\x0D
|                     <img data-bind="visible: smsUnreadCount() > 0 && !showSmsDeleteConfirm()" class="paddingbottom
6" src="./img/sms_unread.png"/>\x0D
|                     <img data-bind="visible: showSmsDeleteConfirm()" class="paddingbottom6" src="./img/sms_full.gi
f"/>\x0D
|                     <sup data-bind="visible: smsUnreadCount() > 0, text: smsUnreadCount" class="smsUnreadCount"></
sup>\x0D
|                 </a>\x0D
|             </span>\x0D
|             <span class="statusItem" title="sim_status" i18n="true" id="statusItemSimStatus"><img data-bind="attr:
{src: simStatus}" class="paddingbottom6"/></span>\x0D
|             <span class="statusItem" title="wifi_status" i18n="true" id="wifi_status" data-bind="visible: hasWifi"
>\x0D
|                 <i class="wifi_status" data-bind="attr:{'class': wifiStatusCssClass}"> </i>\x0D
|             </span>\x0D
|         </div>\x0D
|     </div>\x0D
|     <div id="languageBar" class="row">\x0D
|         <div id="themeContainer" class="col-xs-12 text-right">\x0D
|             <span id="refresh">\x0D
|                 <a class="margin-right-10" id="refreshlink" data-trans="refresh" href="javascript:void(0)" data-bi
nd="click:refresh,visible:showRefresh()" style="display: none;"></a>\x0D
|             </span>\x0D
|             <span id="logout">\x0D
|                 <a class="margin-right-10" id="logoutlink" data-trans="logout" href="javascript:void(0)" data-bind
="click:logout,visible:showLogout() " style="display: none;"></a>\x0D
|             </span>\x0D
|             <span id="login">\x0D
|                 <a class="margin-right-10" id="loginlink" data-trans="login" href="javascript:void(0)" data-bind="
click:login,visible:showLogin() " style="display: none;"></a>\x0D
|             </span>\x0D
|             <!--<select id="language" class="marginright10"></select>-->\x0D
|             <select id="language" class="marginright10" data-bind="value: currentLan, optionsText: 'text', options
Value: 'value', event:{ change: langChangeHandler}">\x0D
|                 <option value="zh-cn" id="language_cn">\xE4\xB8\xAD\xE6\x96\x87</option>\x0D
|                 <option value="en" id="language_en">English</option>\x0D
|                 <option value="el" id="language_el">Espa\xC3\xB1ol</option>\x0D
|             </select>\x0D
|         </div>\x0D
|     </div>\x0D
| </div>\x0D
| <div class="container" class="hide" id="navContainer" style="display: none;">\x0D
```

Accessing the /index.php file directly may reveal source code or other sensitive information, potentially exposing critical system details to unauthorized parties.

Proposed Solution:

Code Review and Patching: Conduct a thorough review of the /index.php file to identify and mitigate any potential vulnerabilities. Apply patches or updates provided by the vendor to address known issues.

Access Control: Implement proper access controls to restrict direct access to sensitive files. Utilize server configurations or authentication mechanisms to prevent unauthorized users from viewing source code or system files.

Security Hardening: Employ server hardening techniques to enhance overall system security. This may include disabling directory listing, restricting file permissions, and implementing web application firewalls (WAFs) to filter and monitor incoming traffic.

Impact:

Unauthorized Access: Malicious actors may gain access to sensitive source code or configurations, leading to potential exploitation and system compromise.

Data Leakage: Exposure of proprietary information or intellectual property could result in reputational damage and financial losses.

Code Execution: Attackers might exploit disclosed source code to identify and exploit additional vulnerabilities within the application or underlying system.

Conclusion:

Addressing the source code disclosure vulnerability (CVE-2010-2333) in the Litespeed Web Server is crucial to safeguarding sensitive information and preventing potential exploitation by malicious actors. By implementing security best practices, such as code review, access control, and system hardening, organizations can mitigate the risk of unauthorized access and protect their assets from compromise.