VULNERABILITY SCANNING - REPORT

MD. ABDULLAH AL NASIR

NETWORK SEURITY [SECTION – B] ID – 19-41052-2

Title: Vulnerability scanning of the target machine is performed by Nessus kali Linux using Metaspoitable 2 VM.

Host Information:

- **Netbios Name**: METASPLOITABLE
- **IP:** 192.168.56.101
- **OS:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Vulnerabilities:

1. **19704 - TWiki 'rev' Parameter Arbitrary Command Execution**.

   Synopsis: The remote web server hosts a CGI application that is affected by an arbitrary command execution vulnerability.

   Description: The version of TWiki running on the remote host allows an attacker to manipulate input to the 'rev' parameter in order to execute arbitrary shell commands on the remote host subject to the privileges of the web server user id.

   See Also http://www.nessus.org/u?c70904f3

   Solution: Apply the appropriate hotfix referenced in the vendor advisory.

   Risk Factor: High

   CVE: CVE-2005-2877

   CVE-2005-2877 – Report: The history (revision control) function in TWiki 02-Sep-2004 and earlier allows remote attackers to execute arbitrary code via shell metacharacters, as demonstrated via the rev parameter to TWikiUsers.

2. **36171 - phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP Code Injection (PMASA-2009-4).**

   Synopsis: The remote web server contains a PHP application that is affected by a code execution vulnerability.

   Description: The setup script included with the version of phpMyAdmin installed on the remote host does not properly sanitize user-supplied input before using it to generate a config file for the application. This version is affected by the following vulnerabilities: - The setup script inserts the unsanitized verbose server name into a C-style comment during config file generation. - An attacker can save arbitrary data to the generated config file by altering the value of the 'textconfig' parameter during a POST request to config.php. An unauthenticated, remote attacker can exploit these issues to execute arbitrary PHP code.

   Solution: Upgrade to phpMyAdmin 3.1.3.2. Alternatively, apply the patches referenced in the project's advisory.

   Risk Factor: High

   CVE: CVE-2009-1285

CVE: CVE-2009-1285 – Report: Static code injection vulnerability in the getConfigFile function in setup/lib/ConfigFile.class.php in phpMyAdmin 3.x before 3.1.3.2 allows remote attackers to inject arbitrary PHP code into configuration files.

3. 136769 - ISC BIND Service Downgrade / Reflected DoS.

Synopsis: The remote name server is affected by Service Downgrade / Reflected DoS vulnerabilities.

Description According to its self-reported version, the instance of ISC BIND 9 running on the remote name server is affected by performance downgrade and Reflected DoS vulnerabilities. This is due to BIND DNS not sufficiently limiting the number fetches which may be performed while processing a referral response. An unauthenticated, remote attacker can exploit this to cause degrade the service of the recursive server or to use the affected server as a reflector in a reflection attack.

Solution: Upgrade to the ISC BIND version referenced in the vendor advisory

Risk Factor: Medium

CVE: CVE-2020-8616

CVE: CVE-2020-8616 – Report: A malicious actor who intentionally exploits this lack of effective limitation on the number of fetches performed when processing referrals can, through the use of specially crafted referrals, cause a recursing server to issue a very large number of fetches in an attempt to process the referral. This has at least two potential effects: The performance of the recursing server can potentially be degraded by the additional work required to perform these fetches, and the attacker can exploit this behavior to use the recursing server as a reflector in a reflection attack with a high amplification factor.