Vulnerability Report

Generated on: 2025-07-12 23:18

Vulnerability Overview

CVE ID	Severity	CVSS	Service	Summary
CVE-2007-4723	High	7.5	Apache httpd	Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache...
CVE-2011-2688	High	7.5	Apache httpd	SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5...
CVE-2009-2299	Medium	5.0	Apache httpd	The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 ...
CVE-2011-1176	Medium	4.3	Apache httpd	The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Mod...
CVE-2009-0796	Low	2.6	Apache httpd	Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Statu...

Detailed Vulnerability Breakdown

IP: 45.33.32.156 | Service: Apache httpd | Version: 2.4.7

CPE: cpe:2.3:a:apache:http_server:2.4.7:*:*:*:*:*:*:*

CVE ID: CVE-2007-4723

Severity: HIGH | CVSS: 7.5

Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

More Info: http://osvdb.org/45879

CVE ID: CVE-2009-0796

Severity: LOW | CVSS: 2.6

Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

More Info: http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html

CVE ID: CVE-2009-2299

Severity: MEDIUM | CVSS: 5.0

Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

More Info: http://secunia.com/advisories/35645

CVE ID: CVE-2011-1176

Severity: MEDIUM | CVSS: 4.3

Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.

More Info: http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=618857

CVE ID: CVE-2011-2688

Severity: HIGH | CVSS: 7.5

Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.

More Info: http://anders.fix.no/software/#unix

Executive Summary & Recommendations

High-Level Overview:

The network's security posture appears to be moderately vulnerable. There are several vulnerabilities identified in the Apache HTTP Server running on port 80 of the IP address 45.33.32.156. The other services running on ports 22, 9929, and 31337 do not have any identified vulnerabilities.

Key Risks by Severity:

1. High Severity: Two high severity vulnerabilities have been identified. CVE-2007-4723 is a directory traversal vulnerability that allows remote attackers to bypass authentication. CVE-2011-2688 is an SQL injection vulnerability that allows remote attackers to execute arbitrary SQL commands.
2. Medium Severity: Two medium severity vulnerabilities have been identified. CVE-2009-2299 can cause a denial of service via an HTTP request with a large Content-Length value but no POST data. CVE-2011-1176 might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.
3. Low Severity: One low severity vulnerability, CVE-2009-0796, has been identified. This is a cross-site scripting vulnerability that allows remote attackers to inject arbitrary web script or HTML.

Recommendations:

1. Patching: Apply the latest patches for the identified vulnerabilities in the Apache HTTP Server. Regularly update and patch all software to minimize the risk of exploitation.
2. Isolation: Consider isolating the Apache HTTP Server from other critical network components to limit the potential impact of a breach.
3. Updates: Update the Apache HTTP Server to the latest version to benefit from the most recent security enhancements.
4. Monitoring: Regularly monitor network traffic for any suspicious activities, particularly on the Apache HTTP Server.

Suspicious or Critical:

The presence of high severity vulnerabilities is critical and requires immediate attention. If left unaddressed, these vulnerabilities could potentially allow an attacker to gain unauthorized access to the system, execute arbitrary commands, or cause a denial of service.