

Vulnerability Report

Generated on: 2025-07-12 23:33

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...
Predicted CPE	High	8.0827	Nping echo	FTP servers can allow an attacker to connect to arbitrary ports on machines other than the...
Predicted CPE	High	7.6830	Nping echo	getcwd() file descriptor leak in FTP....
Predicted CPE	High	7.4929	Nping echo	Remote attackers can cause a denial of service in FTP by issuing multiple PASV commands, c...
Predicted CPE	High	7.3868	Nping echo	Buffer overflow in nftp FTP client version 1.40 allows remote malicious FTP servers to cau...
Predicted CPE	High	7.2829	Nping echo	gFTP FTP client 1.13, and other versions before 2.0.0, records a password in plaintext in ...

CVE-2009-2299	Medium	5.0	Apache httpd	The Artodefence 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>

IP: 45.33.32.156 | Service: Nping echo | Version: Unknown

CPE: New

CVE ID: Predicted CPE

Severity: HIGH | CVSS: 8.0827

Description: FTP servers can allow an attacker to connect to arbitrary ports on machines other than the FTP client, aka FTP bounce.

More Info: Unknown

CVE ID: Predicted CPE

Severity: HIGH | CVSS: 7.6830

Description: getcwd() file descriptor leak in FTP.

More Info: Unknown

CVE ID: Predicted CPE

Severity: HIGH | CVSS: 7.4929

Description: Remote attackers can cause a denial of service in FTP by issuing multiple PASV commands, causing the server to run out of available ports.

[More Info: Unknown](#)

CVE ID: Predicted CPE

Severity: HIGH | CVSS: 7.3868

Description: Buffer overflow in nftp FTP client version 1.40 allows remote malicious FTP servers to cause a denial of service, and possibly execute arbitrary commands, via a long response string.

[More Info: Unknown](#)

CVE ID: Predicted CPE

Severity: HIGH | CVSS: 7.2829

Description: gFTP FTP client 1.13, and other versions before 2.0.0, records a password in plaintext in (1) the log window, or (2) in a log file.

[More Info: Unknown](#)

Executive Summary & Recommendations

High-Level Overview:

The network's security posture is concerning. Several vulnerabilities have been identified across different services, including Apache HTTP Server and Nping echo. These vulnerabilities range from low to high severity, with the majority being high severity.

Key Risks by Severity:

1. High Severity:

- CVE-2007-4723: Directory traversal vulnerability in Apache HTTP Server. This vulnerability could allow remote attackers to bypass authentication.
- CVE-2011-2688: SQL injection vulnerability in Apache HTTP Server. This vulnerability could allow remote attackers to execute arbitrary SQL commands.
- Predicted CPE vulnerabilities in Nping echo: These vulnerabilities could allow remote attackers to connect to arbitrary ports, cause a denial of service, and possibly execute arbitrary commands.

2. Medium Severity:

- CVE-2009-2299 and CVE-2011-1176: These vulnerabilities in Apache HTTP Server could allow remote attackers to cause a denial of service and gain privileges.

3. Low Severity:

- CVE-2009-0796: Cross-site scripting (XSS) vulnerability in Apache HTTP Server. This vulnerability could allow remote attackers to inject arbitrary web script or HTML.

Recommendations:

1. Patching: Apply patches for the identified vulnerabilities in Apache HTTP Server and Nping echo. Regularly check for and apply updates to these services to prevent future vulnerabilities.
2. Isolation: Consider isolating the affected services until the vulnerabilities are patched to prevent potential

exploitation.

3. Updates: Keep all systems and software up-to-date. Regular updates not only provide new features but also fix security vulnerabilities.

4. Monitoring: Regularly monitor network traffic for any suspicious activities. Implement intrusion detection and prevention systems to automatically detect and block potential threats.

Suspicious or Critical:

The presence of high-severity vulnerabilities is critical. If exploited, these could lead to unauthorized access, data loss, or a denial of service. The port 31337 is also suspicious as it is commonly associated with backdoor programs and should be investigated further.