Vulnerability Report

Generated on: 2025-07-10 16:11

IP: 45.33.32.156

Service: OpenSSH

Version: 6.6.1p1 Ubuntu 2ubuntu2.13

CPE: cpe:2.3:a:openbsd:openssh:6.6.1p1:*:*:*:*:*:*

CVE ID: CVE-2007-2768

Severity: MEDIUM | CVSS: 4.3

Description: OpenSSH, when using OPIE (One-Time Passwords in Everything) for PAM, allows remote attackers to determine the existence of certain user accounts, which displays a different response if the user account exists and is configured to use one-time passwords (OTP), a similar issue to CVE-2007-2243.

More Info: http://archives.neohapsis.com/archives/fulldisclosure/2007-04/0635.html

IP: 45.33.32.156

Service: OpenSSH

Version: 6.6.1p1 Ubuntu 2ubuntu2.13

CPE: cpe:2.3:a:openbsd:openssh:6.6.1p1:*:*:*:*:*:*

CVE ID: CVE-2008-3844

Severity: CRITICAL | CVSS: 9.3

Description: Certain Red Hat Enterprise Linux (RHEL) 4 and 5 packages for OpenSSH, as signed in August 2008 using a legitimate Red Hat GPG key, contain an externally introduced modification (Trojan Horse) that allows the package authors to have an unknown impact. NOTE: since the malicious packages were not distributed from any official Red Hat sources, the scope of this issue is restricted to users who may have obtained these packages through unofficial distribution points. As of 20080827, no unofficial distributions of this software are known.

More Info: http://secunia.com/advisories/31575

IP: 45.33.32.156

Service: OpenSSH

Version: 6.6.1p1 Ubuntu 2ubuntu2.13

CPE: cpe:2.3:a:openbsd:openssh:6.6.1p1:*:*:*:*:*:*

CVE ID: CVE-2015-5352

Severity: MEDIUM | CVSS: 4.3

Description: The x11_open_helper function in channels.c in ssh in OpenSSH before 6.9, when ForwardX11Trusted mode is not used, lacks a check of the refusal deadline for X connections, which makes it easier for remote attackers to bypass intended access restrictions via a connection outside of the permitted time window.

More Info: http://lists.opensuse.org/opensuse-security-announce/2015-09/msg00017.html

IP: 45.33.32.156

Service: OpenSSH

Version: 6.6.1p1 Ubuntu 2ubuntu2.13

CPE: cpe:2.3:a:openbsd:openssh:6.6.1p1:*:*:*:*:*:*

CVE ID: CVE-2015-5600

Severity: HIGH | CVSS: 8.5

Description: The kbdint_next_device function in auth2-chall.c in sshd in OpenSSH through 6.9 does not properly restrict the processing of keyboard-interactive devices within a single connection, which makes it easier for remote attackers to conduct brute-force attacks or cause a denial of service (CPU consumption) via a long and duplicative list in the ssh -oKbdInteractiveDevices option, as demonstrated by a modified client that provides a different password for each pam element on this list.

More Info: http://cvsweb.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/auth2-chall.c

IP: 45.33.32.156

Service: OpenSSH

Version: 6.6.1p1 Ubuntu 2ubuntu2.13

CPE: cpe:2.3:a:openbsd:openssh:6.6.1p1:*:*:*:*:*:*

CVE ID: CVE-2015-6563

Severity: LOW | CVSS: 1.9

Description: The monitor component in sshd in OpenSSH before 7.0 on non-OpenBSD platforms accepts extraneous username data in MONITOR_REQ_PAM_INIT_CTX requests, which allows local users to conduct impersonation attacks by leveraging any SSH login access in conjunction with control of the sshd uid to send a crafted MONITOR_REQ_PWNAM request, related to monitor.c and monitor_wrap.c.

More Info: http://lists.apple.com/archives/security-announce/2015/Oct/msg00005.html

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

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-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

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-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

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-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

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-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

Summary & Recommendations

High-Level Overview:

The network security posture is concerning due to the presence of multiple vulnerabilities of varying severity levels. The vulnerabilities are present in OpenSSH and Apache HTTP Server services running on the IP address 45.33.32.156. The Nping echo service and an unidentified service running on port 31337 do not show any known vulnerabilities.

Key Risks by Severity:

1. Critical: CVE-2008-3844 in OpenSSH allows for an externally introduced modification (Trojan Horse) that could have an unknown impact. This vulnerability is critical due to the potential for unauthorized access and control.
2. High: CVE-2015-5600 in OpenSSH can allow remote attackers to conduct brute-force attacks or cause a denial of service (CPU consumption). CVE-2007-4723 and CVE-2011-2688 in Apache HTTP Server are also high severity vulnerabilities that could allow directory traversal and SQL injection attacks respectively.
3. Medium: Several medium severity vulnerabilities exist in both OpenSSH (CVE-2007-2768, CVE-2015-5352) and Apache HTTP Server (CVE-2009-2299, CVE-2011-1176) that could allow attackers to determine the existence of user accounts, bypass intended access restrictions, cause a denial of service, or potentially gain privileges.
4. Low: CVE-2015-6563 in OpenSSH and CVE-2009-0796 in Apache HTTP Server are low severity vulnerabilities that could allow local users to conduct impersonation attacks or remote attackers to inject arbitrary web script or HTML.

Recommendations:

1. Patching: Apply patches for all the identified vulnerabilities in OpenSSH and Apache HTTP Server. If patches are not available, consider upgrading to a newer version of the software that is not vulnerable.
2. Isolation: Isolate the affected systems until the patches or upgrades have been applied to prevent potential exploitation.

3. Updates: Regularly update all software to the latest versions to prevent known vulnerabilities.

4. Regular Scanning: Conduct regular vulnerability scanning to identify and mitigate new vulnerabilities.

Suspicious or Critical:

Port 31337 is traditionally associated with the Back Orifice Trojan, which could indicate a compromised system. It is recommended to investigate this further.