



by **ITrust**
IT SECURITY SERVICES


Security Report

noway.toonux.com

09 January 2014

A graphic of a target with a yellow cone of light and arrows pointing towards the center, overlaid on a network background.

www.ikare-monitoring.com



→ **3.7**

10

noway.toonux.com
88.190.52.71
Debian Linux

0 CRITICAL

0 HIGH

5 MEDIUM

2 LOW

Running Services

Service	Service Name	Risk
General	Linux Kernel	Medium
22/TCP	OpenSSH 5.5p1 Debian 6+squeeze4 (protocol 2.0)	Medium
25/TCP	Postfix smtpd	Medium
80/TCP	Apache httpd	Medium

New Vulnerabilities ordered by port

Service	Name	CVSS	Risk
General/tcp	VSEC Best Practices	6.0	Medium
General/tcp	TCP Sequence Number Approximation Reset Denial of Service Vulnerability	5.0	Medium
General/tcp	TCP timestamps	2.6	Low
22/tcp	Denial of Service in OpenSSH	5.0	Medium
22/tcp	openssh-server Forced Command Handling Information Disclosure Vulnerability	3.5	Low
25/tcp	Check if Mailserver answer to VRFY and EXPN requests	5.0	Medium
25/tcp	SMTP Server type and version	0.0	Info
80/tcp	Apache Web Server ETag Header Information Disclosure Weakness	4.3	Medium
80/tcp	HTTP Bad Method message	0.0	Info
80/tcp	HTTP OPTIONS method	0.0	Info

New Vulnerabilities Description

VSEC Best Practices

Family Name: General Score **CVSS**
6.0

Detected on: **Medium**
88.190.52.71:General/tcp (Jan 09, 2014 03:44:11 PM)

Synopsis :
Ikare run tests to check your compliance to Security Best Practices.

Output:
ssh 88.190.52.71 22 tcp OpenSSH 5.5p1 Debian 6+squeeze4 (protocol 2.0)
smtp 88.190.52.71 25 tcp Postfix smtpd
X509|Certificate signature validity: KO: error 18 at 0 depth lookup:self signed certificate,0
K,,
SSL|Weak algorithms: KO: Accepted weak (40/56 bits) algorithm(s) (respectively 6 & 3)
http 88.190.52.71 80 tcp Apache httpd
HTTP|OPTIONS: Warning: Allowed OPTIONS method

TCP Sequence Number Approximation Reset Denial of Service Vulnerability

Family Name: Denial of Service Score **CVSS**
5.0

Detected on: **Medium**
88.190.52.71:General/tcp (Jan 09, 2014 03:58:04 PM)

Summary:
The host is running TCP services and is prone to denial of service vulnerability.

Insight:
The flaw is triggered when spoofed TCP Reset packets are received by the targeted TCP stack and will result in loss of availability for the attacked TCP services.

Impact:
Successful exploitation will allow remote attackers to guess sequence numbers and cause a denial of service to persistent TCP connections by repeatedly injecting a TCP RST packet.

References:
URL:<http://www.osvdb.org/4030>
URL:<http://xforce.iss.net/xforce/xfdb/15886>
URL:<http://www.us-cert.gov/cas/techalerts/TA04-111A.html>
URL:<http://www-01.ibm.com/support/docview.wss?uid=isgl1Y55949>
URL:<http://www-01.ibm.com/support/docview.wss?uid=isgl1Y55950>
URL:<http://www-01.ibm.com/support/docview.wss?uid=isgl1Y62006>
URL:<http://www.microsoft.com/technet/security/Bulletin/MS05-019.msp>
URL:<http://www.microsoft.com/technet/security/bulletin/ms06-064.msp>
URL:<http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html>
URL:<http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html>
CVE:2004-0230

Solution:
Please see the referenced advisories for more information on obtaining and applying fixes.

Denial of Service in OpenSSH

Family Name: Denial of Service

Score **cvss**

Detected on:

Medium

5.0

88.190.52.71:22/tcp (Jan 09, 2014 03:58:04 PM)

Summary:

Denial of Service Vulnerability in OpenSSH

Insight:

The sshd_config configuration file indicates connection limits:

- *MaxStartups: maximal number of unauthenticated connections (default : 10)*
- *LoginGraceTime: expiration duration of unauthenticated connections (default : 2 minutes)*

However, in this default configuration, an attacker can open 10 TCP sessions on port 22/tcp, and then reopen them every 2 minutes, in order to limit the probability of a legitimate client to a ccess to the service.

Note: MaxStartups supports the 'random early drop' feature, which protects against this type of attack, but it is not enabled by default.

An unauthenticated attacker can therefore open ten connections to OpenSSH, in order to forbid th e access to legitimate users.

This plugin only check OpenSSH version and not test to exploit this vulnerability.

Impact:

Attackers to cause a denial of service (connection-slot exhaustion).

References:

- URL: http://www.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/sshd_config?r1=1.89#rev1.89*
- URL: http://www.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/sshd_config.5?r1=1.156#rev1.156*
- URL: <http://www.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/servconf.c?r1=1.234#rev1.234>*
- URL: <http://vigilance.fr/vulnerability/OpenSSH-denial-of-service-via-MaxStartups-11256>*
- CVE: CVE-2010-5107*

Solution:

Upgrade your OpenSSH to 6.2. or modify LoginGraceTime and MaxStartups on server configuration

Check if Mailserver answer to VRFY and EXPN requests

Family Name: SMTP problems

Score **cvss**

Detected on:

Medium

5.0

88.190.52.71:25/tcp (Jan 09, 2014 03:58:05 PM)

Summary:

The Mailserver on this host answers to VRFY and/or EXPN requests.

VRFY and EXPN ask the server for information about an address. They are inherently unusable through firewalls, gateways, mail exchangers for part-time hosts, etc. OpenVAS suggests that, if you really want to publish this type of information, you use a mechanism that legitimate users actually know about, such as Finger or HTTP.

References:

- URL: <http://cr.yp.to/smtp/vrfy.html>*
- CVE: NOCVE*

Solution:

Disable VRFY and/or EXPN on your Mailserver.

For postfix add 'disable_vrfy_command=yes' in 'main.cf'.

For Sendmail add the option 'O PrivacyOptions=goaway'.

Apache Web Server ETag Header Information Disclosure Weakness

Family Name: Web application abuses

Score **CVSS**

Medium

4.3

Detected on:

88.190.52.71:80/tcp (Jan 09, 2014 03:58:04 PM)

Summary:

A weakness has been discovered in Apache web servers that are configured to use the FileETag directive. Due to the way in which Apache generates ETag response headers, it may be possible for an attacker to obtain sensitive information regarding server files. Specifically, ETag header fields returned to a client contain the file's inode number.

Exploitation of this issue may provide an attacker with information that may be used to launch further attacks against a target network. OpenBSD has released a patch that addresses this issue. Inode numbers returned from the server are now encoded using a private hash to avoid the release of sensitive information.

References:

URL:<https://www.securityfocus.com/bid/6939>

URL:<http://httpd.apache.org/docs/mod/core.html#fileetag>

URL:<http://www.openbsd.org/errata32.html>

URL:<http://support.novell.com/docs/Tids/Solutions/10090670.html>

CVE:CVE-2003-1418

Solution:

OpenBSD has released a patch to address this issue.

Novell has released TID10090670 to advise users to apply the available workaround of disabling the directive in the configuration file for Apache releases on NetWare. Please see the attached Technical Information Document for further details.

openssh-server Forced Command Handling Information Disclosure Vulnerability

Family Name: General

Score **CVSS**

Low

3.5

Detected on:

88.190.52.71:22/tcp (Jan 09, 2014 03:58:04 PM)

Summary:

The `auth_parse_options` function in `auth-options.c` in `sshd` in OpenSSH before 5.7 provides debug messages containing `authorized_keys` command options, which allows remote authenticated users to obtain potentially sensitive information by reading these messages, as demonstrated by the shared user account required by Gitolite. NOTE: this can cross privilege boundaries because a user account may intentionally have no shell or filesystem access, and therefore may have no supported way to read an `authorized_keys` file in its own home directory. OpenSSH before 5.7 is affected

OpenSSH before 5.7 is affected

References:

URL:<http://www.securityfocus.com/bid/51702>

URL:<http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=657445>

URL:<http://packages.debian.org/squeeze/openssh-server>


URL:<https://downloads.avaya.com/css/P8/documents/100161262>

CVE:CVE-2012-0814

Solution:

Updates are available. Please see the references for more information.

TCP timestamps

Family Name: General Score  **2.6**

Detected on: Low **88.190.52.71:General/tcp (Jan 09, 2014 03:58:05 PM)**

Summary:
 The remote host implements TCP timestamps and therefore allows to compute the uptime.


Insight:
 The remote host implements TCP timestamps, as defined by RFC1323.

Impact:
 A side effect of this feature is that the uptime of the remote host can sometimes be computed.

References:
 URL:<http://www.ietf.org/rfc/rfc1323.txt>
 CVE:NOCVE

Solution:
 To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
 To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
 See also: <http://www.microsoft.com/en-us/download/details.aspx?id=9152>

SMTP Server type and version

Family Name: General Score  **0.0**


Detected on: Info **88.190.52.71:25/tcp (Jan 09, 2014 03:58:05 PM)**

Summary:
 This detects the SMTP Server's type and version by connecting to the server and processing the buffer received. This information gives potential attackers additional information about the system they are attacking. Versions and Types should be omitted where possible.

References:
 NOXREF
 CVE:NOCVE

Solution:
 Change the login banner to something generic.

HTTP Bad Method message

Family Name: Web application abuses Score  **0.0**

Detected on: Info **88.190.52.71:80/tcp (Jan 09, 2014 03:58:04 PM)**

Summary:
 HTTP Bad Method message leak same informations than OPTIONS method

Insight:
 The OPTIONS Method provides a list of the methods that are supported by the web server, it represents a request for information about the communication options available on the request/response chain identified by the Request-URI.

Impact:

The *OPTIONS* Method may expose sensitive information that may help an malicious user to prepare more advanced attacks.

References:**URL:**

CVE:NOCVE

Solution:

It's recommended to change the HTTP Bad Method message

HTTP OPTIONS method

Family Name: Web application abusesScore **cvss**

Info

0.0**Detected on:**

88.190.52.71:80/tcp (Jan 09, 2014 03:58:05 PM)

Summary:

HTTP OPTIONS method is enabled on this web server

Insight:

The *OPTIONS* method provides a list of the methods that are supported by the web server, it represents a request for information about the communication options available on the request/response chain identified by the Request-URI.

Impact:

The *OPTIONS* method may expose sensitive information that may help an malicious user to prepare more advanced attacks.

References:**URL:**

CVE:NOCVE

Solution:

It's recommended to disable *OPTIONS* Method on the web server.