www.SecPoint.com - Full Scan Report

Scan Name: CustomerZZ

Audited on May 26, 2014, 2:02 am

Confidential

Introduction

This report is the result of an "online vulnerability assessment scan", performed by **www.SecPoint.com**.

This document has been compiled and arranged to provide a quick and easy-to-understand report to simplify the task of securing computer systems and IT equipment connected to the Internet.

System vulnerabilities are categorised under one of three headings: **High risk, Medium risk or Low risk**.

A detailed explanation of each category of vulnerability can be found under the heading of **Vulnerability Details**

An **Executive Summary** has been compiled specifically for a management level review. This summary contains both written and graphic details based upon the results of the scanner. These results include such information as "when the scan was performed", "who performed the scan", and the amount of system vulnerabilities found in each category.

The **Executive Summary** also includes a conclusion reporting the "overall security level" of the tested system.

Details and names of vulnerabilities discovered are found under the heading of **Summary of vulnerabilities found**. This is followed by individual descriptions for fixing each found vulnerability.

Where possible, a **Bugtraq ID(*)**, a **CVE(**)** and/or a **USN(***)** is present, to verify the existence of the discovered vulnerabilities.

Every system vulnerability discovered is supplied with a possible remedy.

(*) Bugtraq ID is the official Securityfocus.com ID; Also known as bugtraq.
(**) CVE is the official CVE Mitre list.
(***) USN is the official Ubuntu Security Notice list.

Severity Levels

High Risk Vulnerabilities

When a high risk vulnerability is identified, it means that it is possible for an intruder to penetrate and compromise the system fully and/or gain access to highly sensitive system information. This in turn could lead to theft or loss of private and sensitive data.

Medium Risk Vulnerabilities

When a medium Risk vulnerability is identified, it means that an intruder can gain access to system information that could lead to more specific attacks and possibly a full system compromise. This in turn could lead to theft of loss of private or sensitive data.

Low Risk Vulnerabilities

When a low risk vulnerability is identified, it generally means that an intruder can gain access to system information that can aid and lead to more specific attacks resulting in the theft or loss of private and sensitive data.

Information

All entries at this level simply provide additional information to that already available about the current IP. It doesn't imply that the system is vulnerable or not.

Executive Summary

This report represents a security scan performed by **www.SecPoint.com**. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network security.
This scan was performed by user **admin**

Country	IP Number	Started at	Ended at	Duration
United States	XXXXXXXXX	May 26, 2014 02:00:16	May 26, 2014 07:03:29	05:03:13 Hours
Sweden	XXXXXXXX	May 26, 2014 02:00:16	May 26, 2014 06:25:12	04:24:56 Hours

Scan Profile

- Scan Profile for IP 64.79.70.220 : Normal Scan - 10.000 Most Common Ports *RECOMMENDED*
- Scan Profile for IP 90.226.166.216 : Normal Scan - 10.000 Most Common Ports *RECOMMENDED*

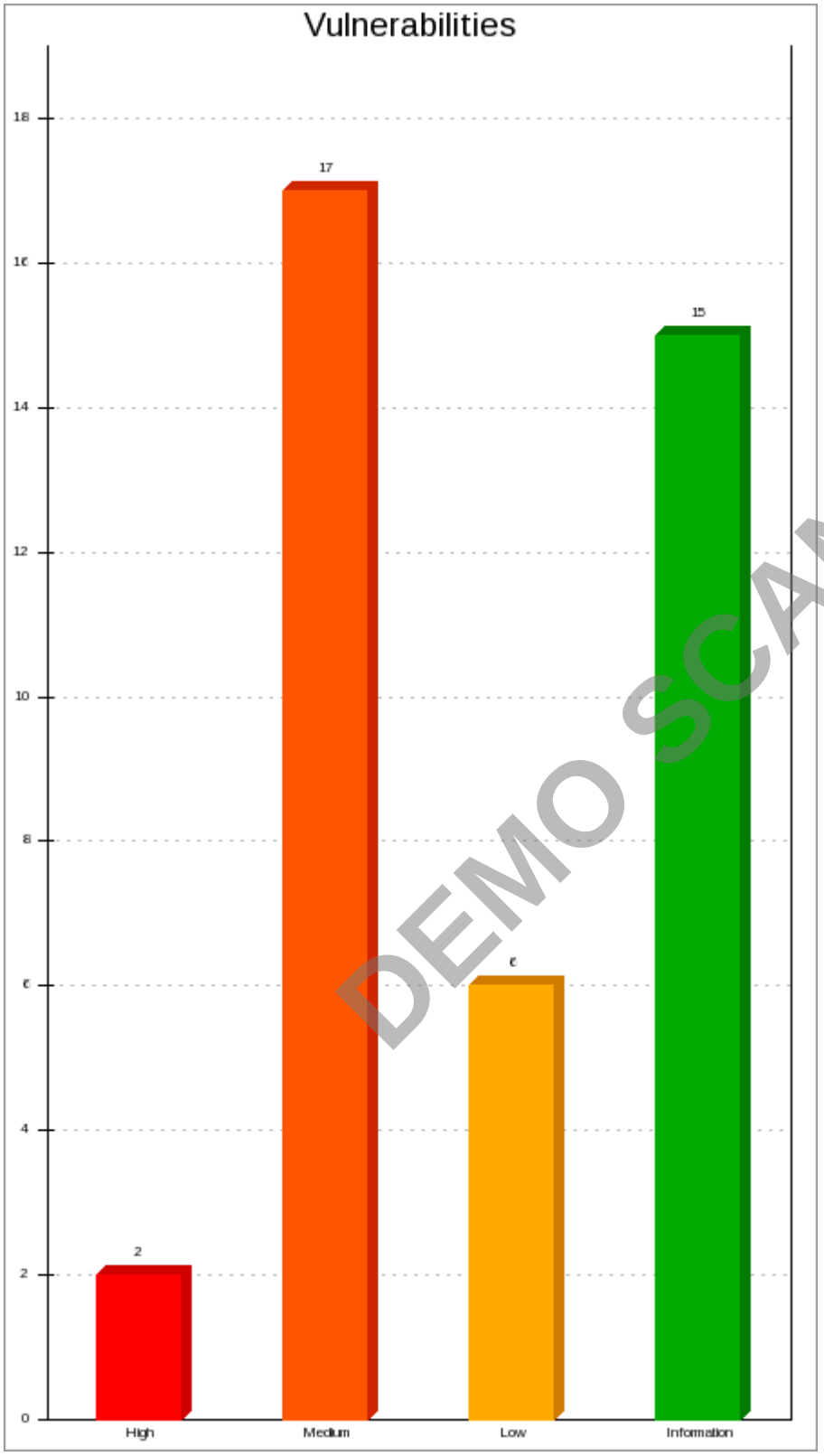
Overall Security Level

Cat 1 (Critical level)

Vulnerabilities

A total of 40, between potential Vulnerabilities and Information, were identified.

They have been categorised as follows: **2 High, 17 Medium, 6 Low, 15 Information.**


Vulnerabilities
18
16
14
12
10
8
6
4
2
0
2
17
6
15
High
Medium
Low
Information

Conclusion

The scan performed by **www.SecPoint.com** has determined that your system security level is dangerously low. It is possible for intruders to fully penetrate the system which can result in loss of private and sensitive data. It is recommended that you take immediate action to improve the security level.

Traceroute

This is the result of a traceroute from www.SecPoint.com to the target IP address:

traceroute to, 15 hops max, 60 byte packets

Hop	Name	IP	Location	Min(ms)	Avg(ms)	Max(ms)	Graph
							0 0
1	ns4.secpoint.com			0.179	0.091	0.089	

A packet filtering device was found protecting the target system typically a firewall system or a router system with ACL (Access Control Lists) set. Even though a filtering device has been found it can still be mis configured and leaving the system vulnerable.

This is the result of a traceroute from to the target IP address:

traceroute to 15 hops max, 60 byte packets

Hop	Name	IP	Location	Min(ms)	Avg(ms)	Max(ms)	Graph
							0 119
1				0.642	0.618	0.840	
2				0.613	0.836	1.101	
3				1.099	1.097	1.097	
4				3.321	3.330	3.327	
5				11.096	11.094	11.093	
6				11.092	10.912	11.124	
7				10.835	10.769	10.850	
8				24.675	37.372	37.312	
9				114.930	114.723	114.919	
10				142.468	117.109	117.056	
11				116.054	116.026	115.984	
12			Sweden	121.180	121.150	118.918	
13			Sweden	117.027	118.340	118.300	
14			Sweden(26) Stockholm	117.183	117.283	117.251	

Identified Ports and Services

The following "Ports and Services" could be identified remotely over the Internet

Ports ad Service for IP:

Port	Protocol	Status	Service
25	tcp	open	Simple Mail Transfer
53	tcp	open	Domain Name Server
80	tcp	open	World Wide Web HTTP
143	tcp	open	Internet Message Access Protocol
443	tcp	open	http protocol over TLS/SSL
587	tcp	open	Submission
993	tcp	open	imap4 protocol over TLS/SSL
8899	tcp	open	ospf-lite

Ports ad Service for IP:

Port	Protocol	Status	Service
443	tcp	open	http protocol over TLS/SSL
8899	tcp	open	ospf-lite

Version Banner identified

The following Service Version Banner outputs were readable remotely over the internet.
It is highly recommended to reconfigure these banners with bogus or no information at all.

Service Version Banner for IP:

Banner name	BIND/NAMED Version Banner
Port	53/udp
Details	Windows Vista
Solution	It is recommended to configure the bind to return bogus information. This can be done by setting the named.conf version "" . If you have already made it return bogus information please ignore this check.

Banner name	SSHd Version Banner
Port	8899/tcp
Details	SSH-2.0-OpenSSH_6.1
Solution	It is highly recommended to configure this output to return bogus or no information at all. If you have done that already please ignore this warning.

Banner name	Smtp Version Banner
Port	25/tcp
Details	220 www.secpoint.com ESMTP
Solution	It is highly adviceable to configure this output to return bogus or no information at all. UNIX: Sendmail;1:Open up the sendmail.cf file;2:Find the line saying O SmtpGreetingMessage= PARAMETERS (Where the parameters can be several $ codes);3:Change the line to O SmtpGreetingMessage=$j (And nothing more). WINDOWS: This is a more complicated process if running exchange and it is therefor recommended to remove at firewall level.;;If you have already removed the version please ignore this warning.

Banner name	Smtp Version Banner
Port	587/tcp
Details	220 ESMTP
Solution	It is highly adviceable to configure this output to return bogus or no information at all. UNIX: Sendmail;1:Open up the sendmail.cf file;2:Find the line saying O SmtpGreetingMessage= PARAMETERS (Where the parameters can be several $ codes);3:Change the line to O SmtpGreetingMessage=$j (And nothing more). WINDOWS: This is a more complicated process if running exchange and it is therefor recommended to remove at firewall level.;;If you have already removed the version please ignore this warning.

Banner name	IMAP Version Banner
Port	143/tcp
Details	* OK [CAPABILITY IMAP4REV1 I18NLEVEL=1 LITERAL+ SASL-IR LOGIN-REFERRALS STARTTLS] www.secpoint.com IMAP4rev1 2007e.404 at Mon, 26 May 2014 02:37:03 +0200 (CEST)
Solution	It is highly adviceable to configure this output to return bogus or no information at all. If you have already done that please ignore this warning.

Service Version Banner for IP:

Banner name	SSHd Version Banner
Port	8899/tcp
Details	SSH-2.0-OpenSSH_5.5
Solution	It is highly recommended to configure this output to return bogus or no information at all. If you have done that already please ignore this warning.

Summary of Vulnerabilities

IP:

High risks vulnerabilities

- Directory // Information Disclosure

- File header.php cluster-E.php Directory Traversal

Medium risks vulnerabilities

- Web Server: Cross Site Scripting

- SSL3_GET_SERVER_CERTIFICATE:certificate verify failed

- Identified Directory /uploads/banners/ Traversal

- Identified /newimages/software/ Directory Traversal

- File /brochure/ Directory Traversal

- File /datasheet/ Directory Traversal

- File /powerpoint/ Directory Traversal

- File /successprogram/ Directory Traversal

- web server /certificates/ directory world readable

- Identified /build/logger/assets/ Directory Traversal

- Identified /build/logger/assets/skins/ Directory Traversal

- Identified /build/logger/assets/skins/sam/ Directory Traversal

- Identified /build/menu/assets/ Directory Traversal

- Identified /build/menu/assets/skins/ Directory Traversal

- Identified /build/menu/assets/skins/sam/ Directory Traversal

- SSH Service Accessible

Low risks vulnerabilities

- PHP Identified

- Read-able /icons/ directory on remote web server software

- Default Apache README File Information Disclosure

- Multiple Files Path Disclosure

- Found /b om remote web server

- RCPT TO: SMTP Service Username Guessing

Information

- All Protocols Tested

- System Time Revealed via. ICMP TimeStamp

- Remote system answers to PING command

- SEO Check Too long IMG ALT/TITLE

- SEO Check Too many tags (>100)

- SEO Check Too many same keywords on a webpage

- SSL Certificate information

- Target SSL Web Server has SSLv3 Enabled

- Mailserver help command found:

- SMTP Ehlo Command

IP:

Medium risks vulnerabilities

- SSH Service Accessible

Information

- All Protocols Tested

- System Time Revealed via. ICMP TimeStamp

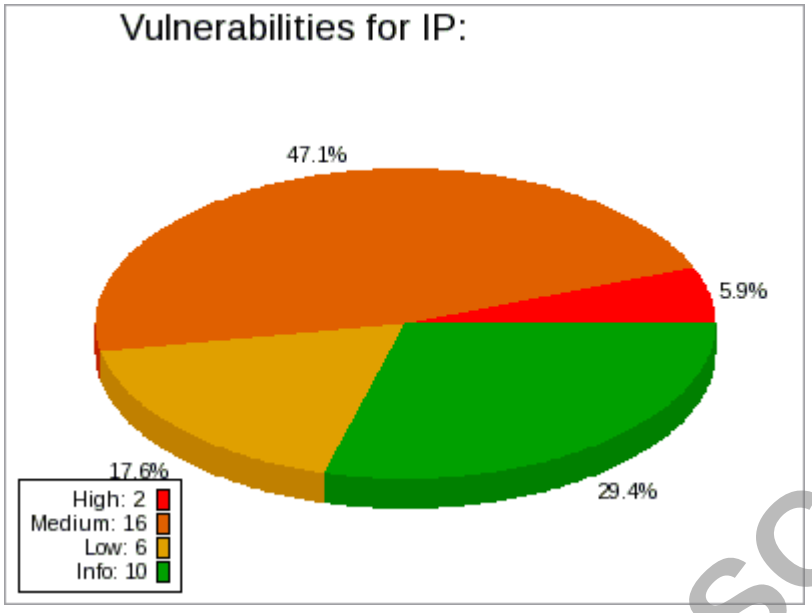
- Remote system answers to PING command

- SSL Certificate information

- Target SSL Web Server has SSLv3 Enabled

Vulnerabilities

Vulnerabilities for IP:



Vulnerability	Directory /js/menu/css/ information Disclosure
Risk Level	High
SecPoint ID	570
Impact	The identified directory found on the remote web server is subject to a remote information disclosure vulnerability. An attacker can use this information to base other attacks on. The service is also running on 80/tcp, 80/tcp, 80/tcp.
Solution	Please upgrade to the latest version of the identified software you are running with the found directory. NOTE: If you are already running the latest version please ignore this check.
Port	80/tcp
Vulnerability output / Evidences	
Evidence: 0	AttackString: GET http:///js/menu/css/ HTTP/1.0
Evidence: 1	AttackOutput: HTTP/1.1 200 OK
Evidence: 2	Vary: Accept-Encoding
Evidence: 3	Cache-Control: max-age=86400
Evidence: 4	Expires: Tue, 27 May 2014 01:07:32 GMT
Evidence: 5	Connection: close
Evidence: 6	Content-Type: text/html
Evidence: 7	<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">

Evidence: 8	<HTML>
Evidence: 9	<HEAD>
Evidence: 10	<TITLE>Index of /js/menu/css</TITLE>
Evidence: 11	</HEAD>
Evidence: 12	<BODY>
Evidence: 13	<H1>Index of /js/menu/css</H1>
Evidence: 14	<PRE><IMG SRC="/icons/blank.gif" ALT=" "> <A HREF="?N=D">Name</A> <A HREF="?M=A">Last modified</A> <A HREF="?S=A">Size</A> <A HREF="?D=A">Description</A>
Evidence: 15	<HR>
Evidence: 16	<IMG SRC="/icons/back.gif" ALT="[DIR]"> <A HREF="/js/menu/">Parent Directory</A> 02-Mar-2014 14:51 -
Evidence: 17	<IMG SRC="/icons/text.gif" ALT="[TXT]"> <A HREF="superfish-navbar.css">superfish-navbar.css</A> 10-Jul-2008 20:41 2k
Evidence: 18	<IMG SRC="/icons/text.gif" ALT="[TXT]"> <A HREF="superfish-vertical.css">superfish-vertical.css</A> 07-Jul-2008 10:31 1k
Evidence: 19	<IMG SRC="/icons/text.gif" ALT="[TXT]"> <A HREF="superfish.css">superfish.css</A> 29-Jan-2011 22:53 4k
Evidence: 20	</PRE><HR>
Evidence: 21	<ADDRESS> Server at <A HREF="mailto:root@secpoint.secpoint.com">www.secpoint.com</A> Port 80</ADDRESS>
Evidence: 22	</BODY></HTML>

Vulnerability	**File header.php cluster-E.php Directory Traversal**
Risk Level	High
SecPoint ID	7639
Impact	The identified file found on the remote web server is subject to a remote Directory Traversal vulnerability. An attacker can exploit this vulnerability to access arbitrary files on the target system. This would be in the contest of the same permissions as of what the web server is running with.
Solution	Please upgrade to the latest version from http://www.npds.org/
Port	80/tcp
Vulnerability output / Evidences	
Evidence: 0	AttackString: GET http:///header.php?Default_Theme=../apache/logs/error.log%00 HTTP/1.0
Evidence: 1	AttackOutput: HTTP/1.1 200 OK
Evidence: 2	Vary: Accept-Encoding

Evidence: 3	Cache-Control: max-age=86400
Evidence: 4	Expires: Tue, 27 May 2014 01:20:19 GMT
Evidence: 5	Connection: close
Evidence: 6	Content-Type: text/html
Evidence: 7	<style>
Evidence: 8	.test a {
Evidence: 9	font-size: 14px !important
Evidence: 10	font-variant: normal
Evidence: 11	font-style: italic
Evidence: 12	font-weight: bold !important
Evidence: 13	test a:hover {
Evidence: 14	color: blue
Evidence: 15	font-weight: bold
Evidence: 16	</style>
Evidence: 17	<table width="100%" cellspacing = "0" cellpadding="0" border="0">
Evidence: 18	<tr><td width="40%"></td>
Evidence: 19	<td width="30%"><form action="http://www.google.com/cse" id="cse-search-box" >
Evidence: 20	<input type="text" name="q" size="22" />
Evidence: 21	<input name="sa" type="submit" class="button2" value="Search" />
Evidence: 22	<input type="hidden" name="cx" value="011570144065842103651:wxfixrdgk2a" />
Evidence: 23	<input type="hidden" name="ie" value="UTF-8" />
Evidence: 24	</form>
Evidence: 25	<script type="text/javascript"src="http://www.google.com/coop/cse/brand?form=cse-search-box&lang=en"></script>
Evidence: 26	<!-- GOOGLE SEARCH FORM END --></td>
Evidence: 27	<td width="25%"><a href="http: border:0
Evidence: 28	><img src="/images/partner_lounge_text.gif" title="Pa

Vulnerability	**Web Server: Cross Site Scripting**
Risk Level	Medium
SecPoint ID	5244
Impact	The identified file found in the VULNOUTPUT section are subject to a remote Cross Site Scripting vulnerability. This can allow an attacker to steal cookie based authentication credentials from the target system.

Solution	Please upgrade to the latest version of the identified file and or if you coded it your self please make input tests on it.
Vulnerability output / Evidences	
Evidence: 0	Possible Cross Site Scripting: (http://php?url=1&sec_code=1&product=&IP=&country=x

Vulnerability	**SSL3_GET_SERVER_CERTIFICATE:certificate verify failed**
Risk Level	Medium
SecPoint ID	56214
Impact	Self-issued or untrusted certificates can't ensure connection details; visitors of the site can't be sure if it is not a fake site/certificate - might be missing chain file
Solution	Consider upgrading your certificate or buying it from well-known issuer
Port	443
Vulnerability output / Evidences	
Evidence: 0	SSL3_GET_SERVER_CERTIFICATE:certificate verify failed

Vulnerability	**Identified Directory /uploads/banners/ Traversal**
Risk Level	Medium
SecPoint ID	49148
Impact	The identified directory found on the remote web server is subject to a remote directory traversal vulnerability. An attacker can exploit this vulnerability to access arbitrary files on the target system in the same permission content as of the web server is running with.
Solution	Please upgrade to the latest version of the identified software you are running with the found directory.
Port	80/tcp
Vulnerability output / Evidences	
Evidence: 0	AttackString: GET http:///uploads/banners/ HTTP/1.0
Evidence: 1	AttackOutput: HTTP/1.1 200 OK
Evidence: 2	Vary: Accept-Encoding
Evidence: 3	Cache-Control: max-age=86400
Evidence: 4	Expires: Tue, 27 May 2014 01:08:28 GMT
Evidence: 5	Connection: close
Evidence: 6	Content-Type: text/html
Evidence: 7	<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
Evidence: 8	<HTML>
Evidence: 9	<HEAD>