

VulnCorp, Inc.

EXTERNAL VULNERABILITY ASSESSMENT AND PENETRATION TEST

AUGUST 1, 2016



PPS Consultant

Project Lead

PPSConsultant@pivotpointsecurity.com



NOTE: The data in this sample report was manufactured to highlight different areas of the report.

The conclusions and recommendations in this report represent the opinions of Pivot Point Security. Determinations of appropriate corrective action(s) are the responsibility of the entity receiving the report.

This report and/or any other materials furnished by Pivot Point Security in connection with this engagement is confidential and may not be duplicated, modified or otherwise reproduced and distributed without the express prior written consent of Pivot Point Security or VulnCorp, Inc. Because this work may contain copyrighted images or other material, permission from the copyright holder may also be necessary if you wish to reproduce.



Table of Contents

SCOPE OF ENGAGEMENT 4

METHODOLOGY 5

 TESTING METHODOLOGY5

 SCORING METHODOLOGY6

VULNERABILITY BENCHMARKING 7

VULNERABILITY VS. RISK 8

HOST RELATIVE VIEW..... 10

 MOST VULNERABLE HOSTS (TOP 10).....10

 MOST AT RISK HOSTS (TOP 10)10

PENETRATION TESTING..... 11

 MANUAL EXPLOITATION EFFORTS (HUMAN-BASED)11

CONCLUSION 20

REMEDIATION 21

SCOPE LIMITATIONS 22

ARTIFACT REMOVAL 23



Scope of Engagement

VulnCorp, Inc. engaged Pivot Point Security (PPS) to conduct a network vulnerability assessment and penetration test against its external Information Technology infrastructure on or about June 17, 2016. The objective of the test was to identify any information system vulnerabilities that may allow levels of un-intended access and provide a measure of the probability that an attacker could exploit these vulnerabilities, and if so, what the impact would be to VulnCorp, Inc. To achieve VulnCorp, Inc.'s requirement for third party attestation of their information security posture, VulnCorp, Inc. determined that the services PPS defines as a Tier 2 Assess level external vulnerability assessment and penetration test would best achieve their requirements.

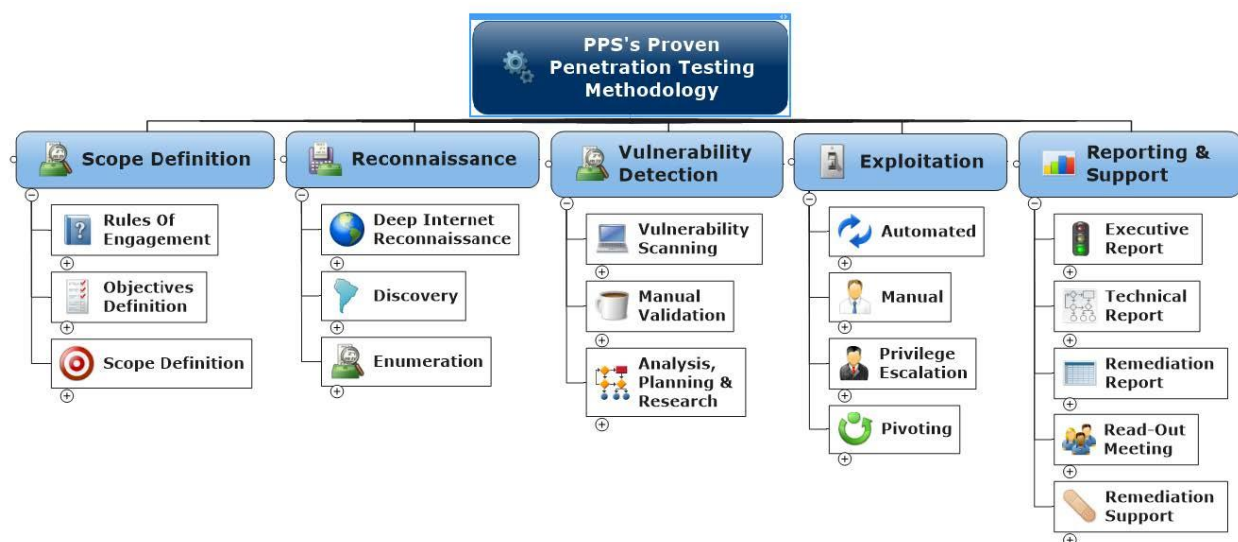
A "Results Details" spreadsheet accompanies this report, which includes the vulnerability details that this report summarizes.



Methodology

Testing Methodology

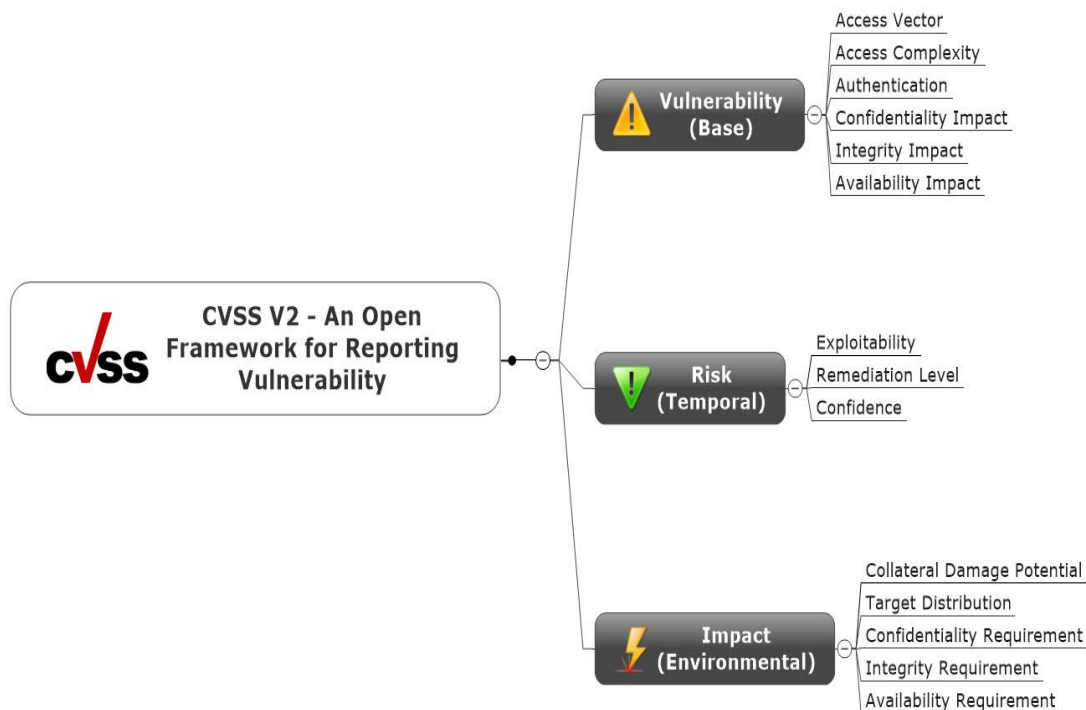
PPS has developed a proven Vulnerability Assessment/Penetration Testing Methodology (illustrated below) from best practices including the Open Source Security Testing Methodology Manual (OSSTMM), the Council for Registered Ethical Security Testers (CREST), the Penetration Testing Execution Standard (PTES), and our 15 plus years of experience. We have also scaled the methodology to account for differing risks and preferred engagement modalities to ensure that we can provide the right testing and assurance at the right cost.





Scoring Methodology

It is important to note that PPS utilizes the Common Vulnerability Scoring System, an open trusted framework that standardizes vulnerability reporting across all major software and hardware platforms. This provides a consistent view of your vulnerability level independent of the company and tools used to perform the assessment.

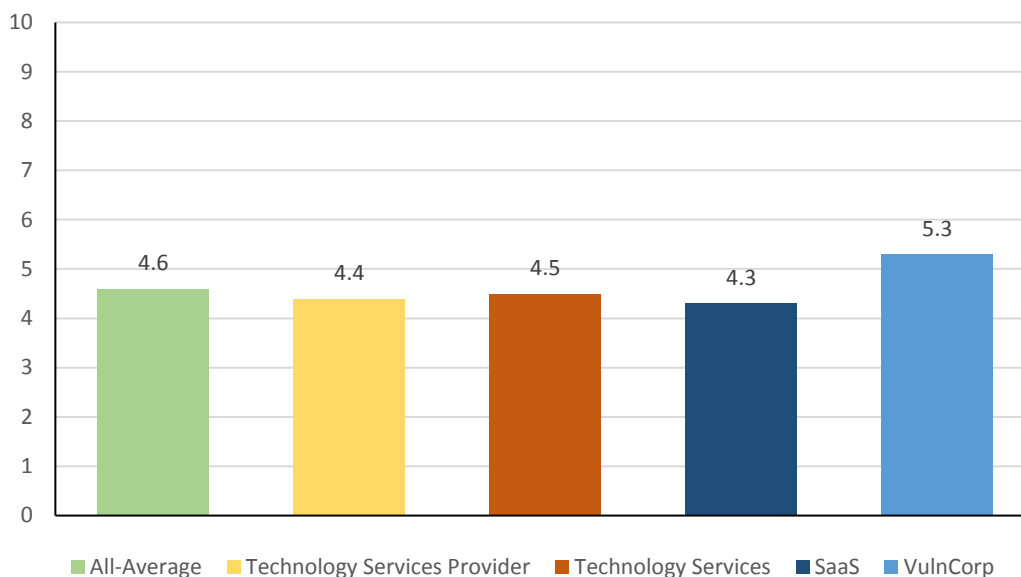


Our testing reports on both the base score and the temporal score. The base (vulnerability) score does not change and references the specific issue discovered; a missing patch for example. The temporal (risk) score can change over time. For example, the temporal score may change if an exploit is released, an official patch becomes available, etc. The third branch (environmental) requires a great deal of business context and is not part of this report.



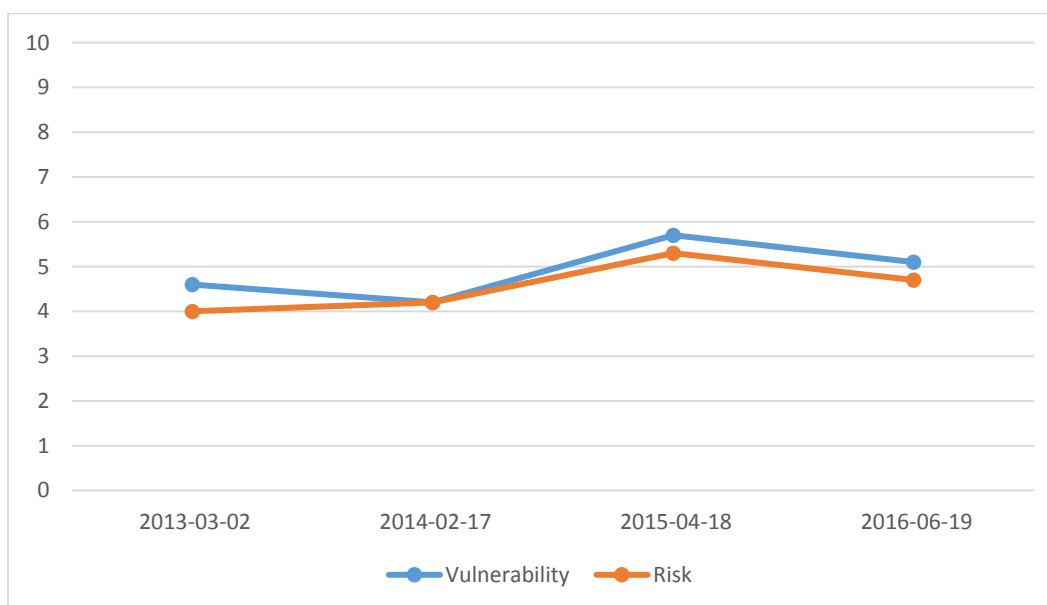
Vulnerability Benchmarking

Pivot Point Security provides a relative benchmark of your vulnerability and risk to other organizations that we have tested at the time of the scan. To derive the score, PPS averages the vulnerability score for each host and then averages all the host scores. For comparison purposes, PPS assigned VulnCorp, Inc. to the "Technical Services" industry, which rolls up into the "Software as a Service" Meta Industry.



Historical Vulnerability/Risk

Pivot Point Security provides a historical view (if available) of vulnerability & risk to gauge the effectiveness of your vulnerability/configuration management practices over time.

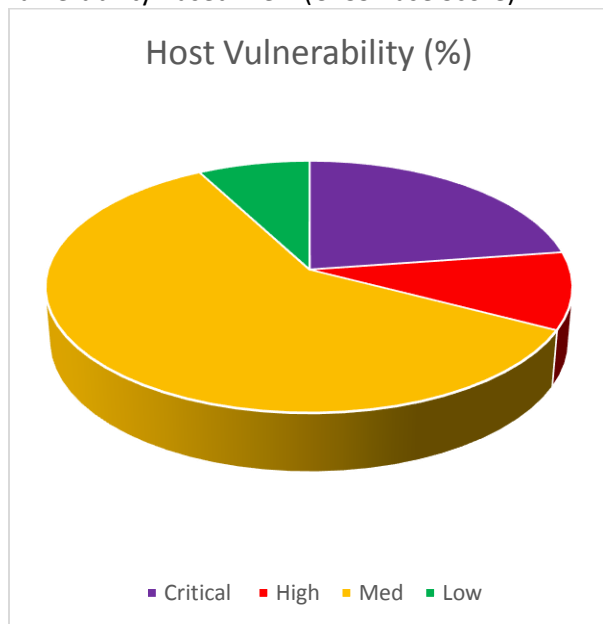




Vulnerability vs. Risk

This host vulnerability chart shows the risk category distribution based on the vulnerability score.

Vulnerability Based View (CVSS Base Score)

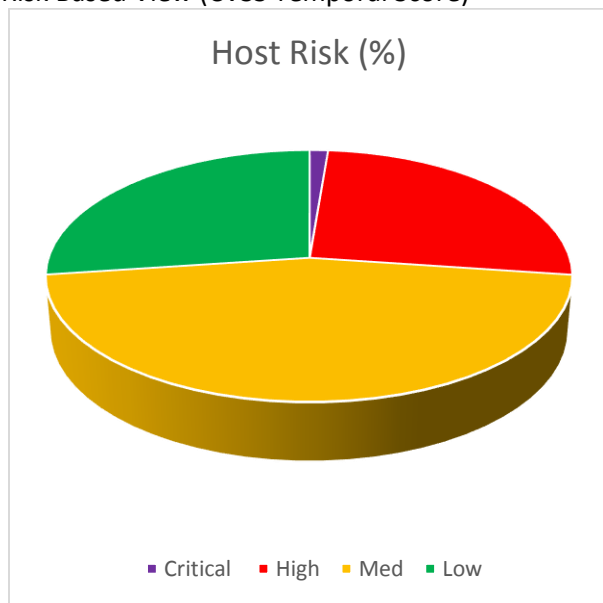


Critical(293)	23%
High(148)	10%
Medium(1453)	60%
Low(10276)	8%

The count is based on Vulnerability x Affected Hosts

This risk level chart takes the temporal score and shows the effective risk level at the time of the testing.

Risk Based View (CVSS Temporal Score)



Critical(15)	1%
High(355)	26%
Medium(915)	46%
Low(10885)	27%

The count is based on Vulnerability x Affected



Host Relative View

Most Vulnerable Hosts (Top 10)

This shows hosts that have the highest level of vulnerability to assist in prioritizing remediation activities (Host Vulnerability = cumulative CVSS Base Score.):

IP Address	Hostname	Host Vulnerability	Critical	High	Medium/Low	% of Org Vulnerability
10.1.1.60		267.3	5	18	13	18%
10.1.1.70		267.3	5	18	13	18%
10.1.1.80	stc-x3650-03.vulncorp.com	267.3	5	18	13	18%
10.1.1.90		267.3	5	18	13	18%
10.1.1.81	stc-x3650.vulncorp.com	144.1	3	6	13	10%
10.1.1.161	stc-vcs-01.vulncorp.com	98.4	2	3	11	7%
10.1.1.151	stc-dc-01.vulncorp.com	68.8	2	1	8	5%
10.1.1.153	stc-dc-02.vulncorp.com	54.5	1	1	7	4%
10.1.1.1		35.4	0	0	7	2%
10.1.1.11		5.8	0	0	1	0%
Total						100%

Most at Risk Hosts (Top 10)

This shows hosts that have the highest level of risk (vulnerability + exploitability + fix ability) to assist in prioritizing remediation activities (Host Risk = cumulative CVSS Temporal Score.):

IP Address	Hostname	Host Risk	Critical	High	Medium/Low	% of Org Risk
10.1.1.60		225.0	1	10	25	15%
10.1.1.70		225.0	1	10	25	15%
10.1.1.80	stc-x3650-03.vulncorp.com	225.0	1	10	25	15%
10.1.1.90		225.0	1	10	25	15%
10.2.1.100		225.0	1	10	25	15%
10.1.1.81	stc-x3650-04.vulncorp.com	124.9	1	4	17	8%
10.1.1.161	stc-vcs-01.vulncorp.com	87.5	0	3	13	5%
10.1.1.165	view-mgr-01.vulncorp.com	70.1	1	1	11	4%
10.1.1.151	stc-dc-01.vulncorp.com	63.7	0	3	8	3%
10.1.1.162	sugarcrm.vulncorp.com	53.7	0	0	11	3%
Total						98%



Penetration Testing

Full data, for all issues and hosts referenced in this narrative, is available in the spreadsheet delivered as part of our reporting. To identify a particular host in the spreadsheet, use the filter/sort/search using the host data referenced in this narrative (e.g., IP Address, Host Name, Host Type, etc.).

Manual Exploitation Efforts (human-based)

On manual review of the vulnerabilities, we found that there were two systems with highly vulnerable web applications running.

Potential Breach Detected

The **app1.vulncorp.com (1.2.3.4)** host requires special attention because the web application manager running on it still has the default administrative password configured. A number of currently deployed applications on this host lead to the suspicion that it was previously compromised. If those applications do not have a legitimate use it is highly recommended to rebuild the system. This will help to ensure that any remnant tools, which could be used to access the system or other network devices, are eliminated. The list of potentially rogue applications has been listed below, as well as the evidence section of the **Apache Tomcat Manager Common Administrative Credentials** vulnerability (*page 11*).



Critical Risk Vulnerabilities

Vulnerability	Count
Unix Operating System on Extended Support	1
Apache Tomcat Manager Common Administrative Credentials	1
Microsoft Windows Server 2003 Unsupported Installation Detection	8

Critical Risk Exploits

Unix Operating System on Extended Support (cvss: 10)

According to its version, the remote host uses a Unix or Unix-like operating system that has reached its end of life. There will be no new security updates issued for this operating system leaving it vulnerable to vulnerabilities discovered after 2016-02-15.

Evidence:

Debian 6.0 support ends on 2014-05-31 end of regular support / 2016-02-15 (end of extended support for Squeeze-LTS).
--

Affected Hosts:

103.192.88.183

Remediation:

Update the host to ensure that the host subscribes to the vendor's extended support plan and continues to receive security updates.

Apache Tomcat Manager Common Administrative Credentials (cvss: 10.0)

We were able to gain access to the Manager web application for the remote Tomcat server using a known set of credentials. A remote attacker can exploit this issue to install a malicious application on the affected server and run arbitrary code with Tomcat's privileges (usually SYSTEM on Windows, or the unprivileged tomcat account on Unix). Worms are known to propagate this way.

Evidence:

It was possible to log into the Tomcat Manager web application using the default username and password. This account had access and privileges to start, stop, and un-deploy all of the running web applications. The account also has permissions to deploy new applications, including those which may contain malicious code. During the investigation, a number of active applications were found that may indicate that the server may have already been compromised (see **Suspicious Web Applications** below).



The server is also hosting a **known-malware web application** called "**JSP RAT by Jeroy**" which allows the user to graphically navigate the servers' filesystem. Other features include file uploads, downloads, editing, and a limited command line access. Read, write, and execute permissions for all functions are limited to the "tomcat" user which does not have administrative access, but can still be very dangerous. Attempts were made to gain deeper access into the system but were unsuccessful. Even so, the ability to view, upload, and execute files means that there is a high risk of privilege escalation.



Suspicious Web Applications

[http:// app1.vulncorp.com:9090/18/](http://app1.vulncorp.com:9090/18/)

[http:// app1.vulncorp.com:9090/rarr/](http://app1.vulncorp.com:9090/rarr/)

<http://app1.vulncorp.com:9090/syadmin/>

The screenshot below shows the Tomcat Web Application manager, after logging in using well-known administrative credentials.



Tomcat Web Application Manager

Message:

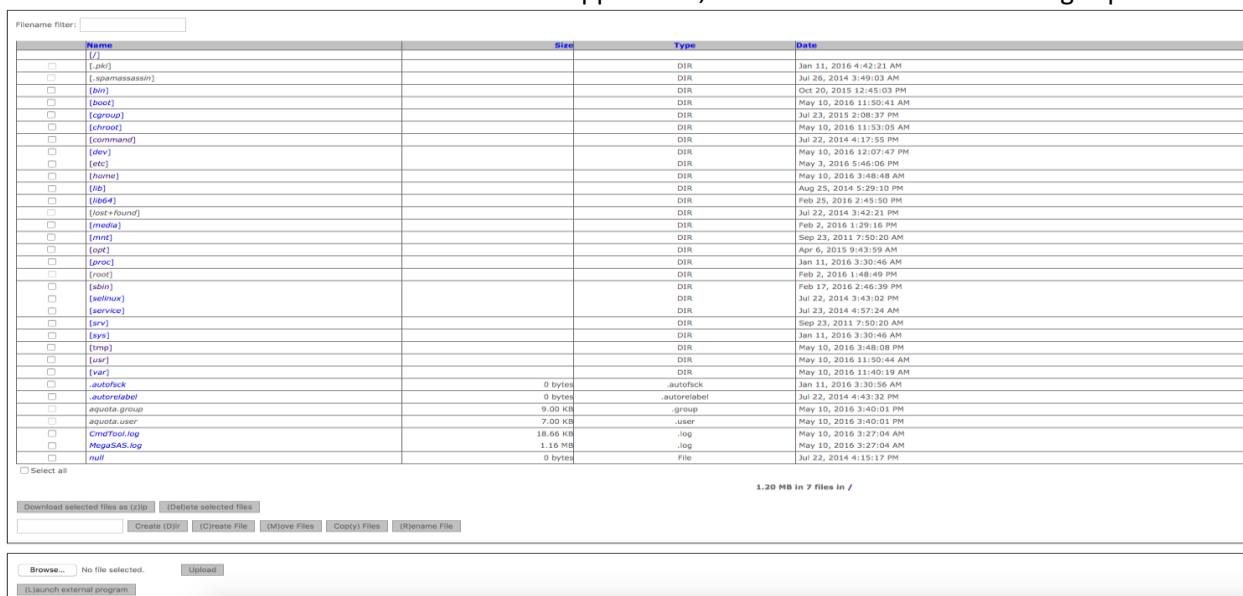
Manager
[List Applications](#) [HTML Manager Help](#) [Manager Help](#) [Server Status](#)

Applications				
Path	Display Name	Running	Sessions	Commands
/	Welcome to Tomcat	true	0	Start Stop Reload Undeploy Expire sessions with idle at 30 minutes
/123		true	0	Start Stop Reload Undeploy Expire sessions with idle at 30 minutes
/18		true	0	Start Stop Reload Undeploy Expire sessions with idle at 30 minutes
/2222		true	0	Start Stop Reload Undeploy Expire sessions with idle at 30 minutes
/888		true	0	Start Stop Reload Undeploy Expire sessions with idle at 30 minutes
/8		true	0	Start Stop Reload Undeploy Expire sessions with idle at 30 minutes
/888		true	0	Start Stop Reload Undeploy Expire sessions with idle at 30 minutes
				Start Stop Reload Undeploy

Screenshot 1 - Tomcat Web Application Manager (post-login)



This is a screenshot from the **JSP RAT** malware application, which shows the file-browsing capabilities.



Screenshot 2 - File browser

Affected Hosts:

app1.vulncorp.com

Remediation:

Edit the associated tomcat-users.xml file and change or remove the affected set of credentials. Also remove any rogue applications (such as **JSP RAT**).

SPECIAL NOTE: Given that this host appears to have already been compromised, it is advisable to re-build the system. This will help to ensure that any backdoors left by attackers will be removed.

Microsoft Windows Server 2003 Unsupported Installation Detection (cvss: 10.0)

The remote host is running Microsoft Windows Server 2003. Support for this operating system by Microsoft ended July 14, 2015.

Lack of support implies that the vendor will not release any new security patches for the product. As a result, it is likely to contain security vulnerabilities. Furthermore, Microsoft is unlikely to investigate or acknowledge reports of vulnerabilities.

Evidence:

It is possible that there are unpublished/undiscovered vulnerabilities that an attacker could use to easily gain access to any systems running Windows Server 2003.



Affected Hosts:

213.235.154.243, 206.231.224.127, 79.242.80.70, 125.1.169.185, 5.18.159.164, 201.15.116.84,
130.145.72.121, 79.224.109.204

Remediation:

Upgrade to a version of Windows that is currently supported.



High Risk Vulnerabilities

Vulnerability	Count
PHP 5.3.x < 5.3.29 Multiple Vulnerabilities	7
OpenSSL ChangeCipherSpec MiTM Vulnerability	10
OpenSSL Heartbeat Information Disclosure (Heartbleed)	3

High Risk Exploits

PHP 5.3.x < 5.3.29 Multiple Vulnerabilities (cvss: 7.5)

According to its banner, the version of PHP installed on the remote host is 5.3.x prior to 5.3.29. It is, therefore, affected by the following vulnerabilities:

- A heap-based buffer overflow error exists in the file ext/date/lib/parse_iso_intervals.c related to handling DateInterval objects that allows denial of service attacks. (CVE-2013-6712)
- A boundary checking error exists related to the Fileinfo extension, Composite Document Format (CDF) handling, and the function cdf_read_short_sector. (CVE-2014-0207)
- A flaw exists with the cdf_unpack_summary_info() function within src/cdf.c where multiple file_printf calls occur when handling specially crafted CDF files. This could allow a context dependent attacker to crash the web application using PHP. (CVE-2014-0237)
- A flaw exists with the cdf_read_property_info() function within src/cdf.c where an infinite loop occurs when handling specially crafted CDF files. This could allow a context dependent attacker to crash the web application using PHP. (CVE-2014-0238)
- A type-confusion error exists related to the Standard PHP Library (SPL) extension and the function unserialize. (CVE-2014-3515)
- An error exists related to configuration scripts and temporary file handling that could allow insecure file usage. (CVE-2014-3981)
- A heap-based buffer overflow error exists related to the function dns_get_record that could allow execution of arbitrary code. (CVE-2014-4049)
- An out-of-bounds read exists in printf. (Bug #67249)

Note that Nessus has not attempted to exploit these issues, but has instead relied only on the application's self-reported version number. Additionally, note that version 5.3.29 marks the end of support for the PHP 5.3.x branch.



Evidence:

```
Version source      : Server: Apache/2.2.21 (win32) mod_ssl/2.2.21  
OpenSSL/1.0.0e PHP/5.3.8 mod_perl/2.0.4 Perl/v5.10.1  
Installed version  : 5.3.8  
Fixed version      : 5.3.29
```

PPS did not attempt to test this exploit since it has a very high risk of creating a Denial-of-Service (DoS) condition. However, it is still possible that an attacker may use this vulnerability to intentionally take down services.

Affected Hosts:

28.102.41.93, 54.147.117.243, 201.15.116.84, 130.145.72.121, 17.64.3.212, 237.21.37.52

Remediation:

Upgrade to PHP version 5.3.29 or later.

*Medium Risk Vulnerabilities*

Vulnerability	Count
SSL RC4 Cipher Suites Supported (Bar Mitzvah)	10
SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	9
SSL Version 2 and 3 Protocol Detection	9
SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened encryption)	3
SSL Certificate Cannot Be Trusted	10
SSL Self-Signed Certificate	10
SSH Weak Algorithms Supported	1
SSL Certificate with Wrong Hostname	2
SMB Signing Disabled	2
DNS Server Spoofed Request Amplification DDoS	1

Medium & Low Risk Exploits

SSL RC4, SSL v2, SSL v3, and SSH Weak Algorithms

The SSL/TLS implementation of the RC4 algorithm contains a bug where it does not handle session state and key data in a secure manner. Anyone that is sniffing the network traffic when a session is started can use a combined weak key/brute-force attack to decrypt the session data.

SSL Version 2, which has not been updated since the release of SSL version 3 (c. 1996), contains numerous security deficiencies including the use of the weak MD5 encryption method, and other flaws that allow for Man-in-the-Middle¹ (MitM) attacks. Successful MitM attacks can then be used to manipulate the SSL session data and even terminate it without either side knowing if the session ending was for legitimate reasons.

SSL Version 3 encrypts all of its traffic with either RC4 or a block cipher in CBC mode; both are known to have security issues. If a malicious individual were able to insert themselves between the SSL client and server (Man-in-the-Middle), they would be able to capture enough data from repeated transmissions of either passwords or HTTP cookies, that they would be able to decrypt the traffic back into plain text. Because there are no workarounds for this issue, SSL v3 needs to be removed as an option.

Weak algorithms, such as RC4 and MD5, are problematic because they have known issues that can be used as part of an attack to decrypt the otherwise-protected data. Such attacks may have pre-requisites such as being able to sniff traffic between two systems, i.e. someone on the network, but others might simply require a strongly motivated individual to configure a system to perform a mathematical brute-force attack against a particular block of data. Regardless of the requirements, the use of weak algorithms is ill advised because their flaws may be used to expose sensitive information.

¹ A Man-in-the-Middle attack is one whereby an attacker is able to act as a go-between for all traffic between a server and a client. In doing so they imitate both sides of the conversation and manipulate data as they see fit.



Invalid SSL Certificates

SSL certificates are used by the web server in two ways. The first way is to establish a secure channel for transmitting data to and from a web browser. If the encryption used during this communication is weakened by allowing vulnerable encryption methods, then any attacker willing to employ considerable resources may be able to decrypt and gain access to any data that was previously encrypted by that web server.

The second way that SSL certificates are used is identity verification. Having a valid certificate means that a 3rd party can attest to the fact that a device or service is indeed who they say they are. Hosts with invalid or self-signed certificates create an opening for a malicious individual to redirect or intercept user traffic because there is no way to prove that they are not legitimate.

SMB Signing Disabled

The Server Message Block (SMB) protocol is used to provide access to shared files, printers, serial ports, and transmit other messages between hosts on a network. Since these messages may contain sensitive information or be used to send control messages, verifying the source of the SMB message becomes very important. This verification is done by using digital signatures. Without message signing, anyone with access to the network may be able to craft their own unsigned SMB packets or MiTM them to gain access to files or obtain sensitive information.

DNS Server Spoofed Request Amplification DDoS

One or more name servers in the tested network responded to a "." query which provided all available information about the DNS root zone. Because the volume of data contained in the response was exponentially larger (by a factor of about 30) than the initial request, a malicious individual could send the same request repeatedly thereby flooding the network and preventing other traffic from flowing. This is known as a Denial-of-Service (DoS) attack. The amplification in the issue heading comes from the fact that the query is smaller than the response. In other words, 17 bytes of data becomes amplified into 449 bytes of data.

Not having any other viable attack modalities likely to yield unintended access, we terminated testing.



Conclusion

PPS determined that the network tested was not secured in a manner aligned with good practice. There were a number of issues identified that negatively impact the security posture of VulnCorp Inc. For example; Services with default credentials and unsupported operating systems were discovered, as well as a number of machines with insecure configurations and/or missing patches.



Remediation

- Upgrade or retire systems running unsupported operating systems and software.
 - Debian 6
 - Extended/Long-term Support for this system ended on February 15, 2016. Performing a distribution upgrade to a supported version is recommended. Versions that also include extended/long-term support are preferable.
 - Windows 2003 Server
 - Support ended in June 14th, 2015 for Windows Server 2003. All systems should be retired or upgraded to a support version.
- Patch Management review
 - Ensure your patch management program accounts for all systems and devices.
 - Ensure missing patches are tested and deployed on all systems.
 - For example:
 - PHP 5.3.x < 5.3.29 (Multiple Vulnerabilities)
 - Currently installed versions of PHP contain multiple vulnerabilities that an attacker could potentially use to crash/destabilize services. Exploiting these service-crash vulnerabilities may also provide arbitrary code execution.
- Insecure Configuration
 - SSL/TLS, SSH (Multiple Vulnerabilities)
 - There are a number of SSL/TLS-related items which need to be addressed. These issues primarily fall into either the weak encryption or identity spoofing categories. While these issues generally require a concerted and often long-term effort on the part of an attacker, they are still possible ways in which sensitive information may be leaked/compromised.
 - Ensure that SSL enabled services use valid SSL certificates.
 - Do not allow SSLv2 and SSLv3 connections. Restrict access to TLS 1.2 if possible.
 - Remove support for weak cryptographic ciphers and weak key strength ciphers
 - SMB Signing Disabled
 - Digitally signing SMB messages will help to ensure that malicious individuals are unable to craft packets to obtain information or gain unauthorized access to a resource.
 - Enable signing of all SMB messages.
 - DNS Server Spoofed Request Amplification DDoS
 - Servers that provide DNS can be easy targets for Denial-of-Service attacks (distributed or otherwise). However, making sure to configure these systems per-industry best-practices is often the simplest way to mitigate issues.
 - Disable responses to DNS root/"." queries, and/or limit DNS access from external systems



Scope Limitations

Man-in-the-Middle (MitM) attacks and “brute force” attacks which can be used to gain access to credentials, decrypt encrypted data, and/or access clear text data are outside the scope of the contracted testing as they can be time consuming, difficult to execute in a “true-to-life” manner, and provide little substantive value (as their exploitability is well documented).

All hosts provided to Pivot Point Security (PPS) were considered to be in scope in terms of scanning, and penetration testing. Efforts were made by PPS to minimize impact to client sites. Vulnerabilities which require brute force or include any risk of crashing an application, service, or host were detected but not tested.



Artifact removal

Included below is a list of testing artifacts that systems administrators should search for and remove from each system, as the automated tool may not have removed them.

There are no artifacts that need to be cleaned up.