



PCI Audit Report

Certified PCI Report for Hoyt LLC

Audited on May 03 2010

Reported on May 03 2010

Table of Contents

1 Scanned Hosts and Networks
2 PCI Scoring System
3 Vulnerabilities by IP Address and PCI Severity Level
3.1 209.251.180.146
4 Vulnerability Details
4.1 Medium (2)
4.2 Low (1)
5 Vulnerability Exceptions

1. Scanned Hosts and Networks

The following hosts/networks were scanned. Devices that were not found to be active (did not respond to network traffic) are not included in the remainder of this report.

- www.hoyt.net

2. PCI Scoring System

This report is approved for use in Payment Card Industry (PCI) audits, according to the PCI Data Security Standard (DSS) Version 1.2.

A PCI network audit produces one of two possible results.

- **PASSED** indicates that the network is compliant with the PCI DSS.
- **FAILED** indicates that the network is not compliant with the PCI DSS.

The ASV bases the audit result on a score that is calculated for every vulnerability. The framework for this calculation, as required by the PCI DSS, is the Common Vulnerability Scoring System (CVSS), Version 2. CVSS scores range from 0 to 10.0, with 4.0 or higher indicating failure to comply with PCI standards.

A CVSS score is a computation of base metrics that reflect how much risk a vulnerability poses to network security. Base metrics include access (ranging from local to remote), access complexity, required authentication, impact on data confidentiality, impact on data integrity, and impact on data availability.

For vulnerabilities that are not defined according to the CVSS, NeXpose uses the legacy PCI scoring system, as sanctioned by the PCI DSS. This system ranks vulnerabilities on a severity scale from 1 to 5. Any vulnerability ranking above 2 indicates failure to comply with PCI standards.

Level 5 vulnerabilities permit attacks with remote root or remote administrator capabilities that can compromise an entire host.

Level 4 vulnerabilities permit attacks with remote user capabilities and partial file system access.

Level 3 vulnerabilities permit access to specific stored information, such as security settings.

Level 2 vulnerabilities expose some sensitive host information, such as precise versions of services.

Level 1 vulnerabilities expose information such as open ports.

NeXpose follows additional PCI compliance guidelines as stated in the PCI DSS Technical and Operational Requirements for Approved Scanning Vendors (ASVs):

"If a CVSS base score is not available for a given vulnerability identified in the component, then the compliance criteria to be used by the ASV is the possibility of the identified vulnerability leading to a data compromise."

Also, any vulnerability leading to XSS or SQL injection will indicate failure, regardless of CVSS score.

3. Vulnerabilities by IP Address and PCI Severity Level

3.1. 209.251.180.146

PCI Compliance Status	PASSED
Operating System	Microsoft Windows
Aliases	STALKER, www.hoyt.net

Vulnerability	Severity	PCI Compliance Status	Port	Status	Additional Information
A service discloses version information	Medium (2)	Passed	1433/tcp	Exploited	TDS on TCP port 1433 running SQL Server 2008 10.0.2531
A service discloses version information	Medium (2)	Passed	9982/tcp	Exploited	HTTPS on TCP port 9982 running Microsoft-IIS 7.0
ASP.NET Detailed Error Message Information Leak	Medium (2)	Passed	9981/tcp, 9982/tcp, 9983/tcp	Exploited	
Microsoft IIS Authentication Method Disclosure	Medium (2)	Passed	9981/tcp	Exploited	CVE-2002-0419
A running service was discovered	Low (1)	Passed	21/tcp	Exploited	FTP on TCP port 21
A running service was discovered	Low (1)	Passed	25/tcp	Exploited	SMTP on TCP port 25
A running service was discovered	Low (1)	Passed	80/tcp	Exploited	HTTP on TCP port 80
A running service was discovered	Low (1)	Passed	143/tcp	Exploited	IMAP on TCP port 143
A running service was discovered	Low (1)	Passed	389/tcp	Exploited	LDAP on TCP port 389
A running service was discovered	Low (1)	Passed	443/tcp	Exploited	HTTPS on TCP port 443
A running service was discovered	Low (1)	Passed	990/tcp	Exploited	FTPS on TCP port 990
A running service was discovered	Low (1)	Passed	993/tcp	Exploited	IMAP on TCP port 993
A running service was discovered	Low (1)	Passed	1433/tcp	Exploited	TDS on TCP port 1433
A running service was discovered	Low (1)	Passed	3389/tcp	Exploited	Microsoft Remote Display Protocol on TCP port 3389
	Low (1)	Passed	8443/tcp	Exploited	HTTPS on TCP port 8443

Vulnerability	Severity	PCI Compliance Status	Port	Status	Additional Information
A running service was discovered					
A running service was discovered	Low (1)	Passed	9981/tcp	Exploited	HTTPS on TCP port 9981
A running service was discovered	Low (1)	Passed	9982/tcp	Exploited	HTTPS on TCP port 9982
A running service was discovered	Low (1)	Passed	9983/tcp	Exploited	HTTPS on TCP port 9983

3.1.1. Remediation Overview for 209.251.180.146

For Microsoft IIS

The Microsoft IIS vulnerabilities can be resolved by performing the following 2 steps. The total estimated time to perform all of these steps is 28 hours 20 minutes.

Remediation Step	Estimated Time
<p>Disable detailed ASP.NET error reporting in IIS</p> <p>Follow Microsoft's detailed instructions in knowledgebase article 306355 to disable detailed ASP.NET error messages using either custom error pages or the root-level Web.config file.</p> <p>This must be applied for the following issues:</p> <ul style="list-style-type: none"> •/%3f.jsp •/%3f.jsp%5C •/ScriptResource.axd •/ScriptResource.axd •/Trace.axd •/Trace.axd •/WebResource.axd •/WebResource.axd •/default.aspx%3f.jsp •/images/Trace.axd •/javascript/Trace.axd •/log/Trace.axd •/scripts/%3f.jsp •/scripts/Trace.axd 	28 hours
<p>Fix Microsoft IIS Authentication Method Disclosure</p> <p>If the server is intended for public use then it may be possible to simply disable both basic and integrated Windows authentication. Sites that use form-based logins when users are authenticated against a database and track logged in users with cookies will be able to disable these authentication methods. Doing this will prevent such attacks.</p> <p>If basic or integrated Windows authentication is required on the server, these steps should be considered: Set</p>	20 minutes

Remediation Step	Estimated Time
the account lockout threshold to help minimize the risk of successful brute force attacks. Using the "passprop" utility it is possible to enable account lockout for the default "administrator" account. Rename the administrator account if this has not already been done.	

For Microsoft-IIS 7.0

The Microsoft-IIS 7.0 vulnerabilities can be resolved with a single step. The estimated time to perform this step is 6 hours.

Remediation Step	Estimated Time
<p>Disable detailed ASP.NET error reporting in IIS Follow Microsoft's detailed instructions in knowledgebase article 306355 to disable detailed ASP.NET error messages using either custom error pages or the root-level Web.config file.</p> <p>This must be applied for the following issues:</p> <ul style="list-style-type: none">•/ScriptResource.axd•/Trace.axd•/WebResource.axd	6 hours

4. Vulnerability Details

4.1. Medium (2)

Level 2 vulnerabilities expose some sensitive information from the host, such as precise versions of services. With this information, hackers could research potential attacks to try against a host.

4.1.1. A service discloses version information (generic-service-version-disclosure)

Severity	Medium (2)
Category	Information Gathering
CVSS score	4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)
Affects	209.251.180.146

Description

A service was found to be running that provides detailed version information. This information can be used to determine what vulnerabilities may exist in the service, assisting malicious users in launching more targeted attacks.

Solution

Disable or obfuscate the version information returned by the service, if possible.

4.1.2. ASP.NET Detailed Error Message Information Leak (http-asp-dot-net-errmsgs-enabled)

Severity	Medium (2)
Category	Web
CVSS score	5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
Affects	209.251.180.146
References	URL: http://www.owasp.org/index.php/Error_Handling,_Auditing_and_Logging#Detailed_error_messages , URL: http://support.microsoft.com/kb/306355 , URL: http://www.microsoft.com/technet/technetmag/issues/2006/11/InsideMSCOM/

Description

A detailed ASP.NET error message was discovered. Detailed error messages can include diagnostics, path and OS information, software versions, and other sensitive information of use to attackers.

Solution

Follow Microsoft's detailed instructions in knowledgebase article [306355](http://support.microsoft.com/kb/306355) to disable detailed ASP.NET error messages using either custom error pages or the root-level Web.config file.

4.1.3. Microsoft IIS Authentication Method Disclosure ([http-iis-auth-method-disclosure](#))

Severity	Medium (2)
Category	Microsoft IIS, Web, Windows
CVSS score	5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
Affects	209.251.180.146
References	CVE-2002-0419 , BID: 4235

Description

Microsoft IIS supports Basic and NTLM authentication. The authentication methods supported by a given IIS server can be revealed to an attacker through the inspection of returned error messages, even when anonymous access is also granted.

When a valid authentication request is submitted for either message with an invalid username and password, an error message will be returned. This happens even if anonymous access to the requested resource is allowed. An attacker may be able to use this information to launch further intelligent attacks against the server, or to launch a brute force password attack against a known user name.

Solution

If the server is intended for public use then it may be possible to simply disable both basic and integrated Windows authentication. Sites that use form-based logins when users are authenticated against a database and track logged in users with cookies will be able to disable these authentication methods. Doing this will prevent such attacks.

If basic or integrated Windows authentication is required on the server, these steps should be considered:

- Set the account lockout threshold to help minimize the risk of successful brute force attacks. Using the "passprop" utility it is possible to enable account lockout for the default "administrator" account.
- Rename the administrator account if this has not already been done.

4.2. Low (1)

Level 1 vulnerabilities are information such as open ports.

4.2.1. A running service was discovered (generic-service-open)

Severity	Low (1)
Category	General Remote Services
Affects	209.251.180.146

Description

A service was found to be running on the system.

Solution

If the service is not required for normal business operations, it should be disabled. Leaving unnecessary services running on a system provides malicious users with additional attack vectors when attempting to compromise a system.

5. Vulnerability Exceptions

Vulnerability	Severity	Reason	Authorization	Comments	Affects
MS09-048: Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution	Critical	False Positive	jjames on 2010-05-03	see case 33676	209.251.180.146
MS09-061: Vulnerabilities in the Microsoft .NET Common Language Runtime Could Allow Remote Code Execution	Critical	False Positive	jjames on 2010-04-30	see case 33676	209.251.180.146
MS09-062: Vulnerabilities in GDI+ Could Allow Remote Code Execution	Critical	False Positive	jjames on 2010-05-03	see case 33676	209.251.180.146
MS08-001: Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (941644)	Critical	False Positive	jjames on 2010-04-30	see case 33676	209.251.180.146
TLS Session Renegotiation Vulnerability	Severe	False Positive	jjames on 2010-04-30	see case 33676	209.251.180.146
MS08-036: Vulnerabilities in Pragmatic General Multicast (PGM) Could Allow Denial of Service (950762)	Severe	False Positive	jjames on 2010-05-03	see case 33676	209.251.180.146
MS08-037: Vulnerabilities in DNS Could Allow Spoofing (953230)	Severe	False Positive	jjames on 2010-04-30	see case 33676 using SimpleDNS confirmed by vendor it is a False Positive.	209.251.180.146
Microsoft RDP Protocol Hard-coded RSA Private Key Weakness	Severe	False Positive	jjames on 2010-04-30	see case 33676	209.251.180.146

PCI Audit Report

Vulnerability	Severity	Reason	Authorization	Comments	Affects
TLS/SSL Server Supports Weak Cipher Algorithms	Severe	False Positive	jjames on 2010-04-30	See case 33676	209.251.180.146
TCP Sequence Number Approximation Vulnerability	Severe	False Positive	jayel on 2010-02-24	See case 32284 for evidence.	209.251.180.146
TCP Sequence Number Approximation Vulnerability	Severe	False Positive	jayel on 2010-02-24	See case 32284 for evidence.	209.251.180.146
TCP Sequence Number Approximation Vulnerability	Severe	False Positive	jayel on 2010-02-24	See case 32284 for evidence.	209.251.180.146
TCP Sequence Number Approximation Vulnerability	Severe	False Positive	jayel on 2010-02-24	See case 32284 for evidence.	209.251.180.146
TCP Sequence Number Approximation Vulnerability	Severe	False Positive	jayel on 2010-02-24	See case 32284 for evidence.	209.251.180.146
TCP Sequence Number Approximation Vulnerability	Severe	False Positive	jayel on 2010-02-24	See case 32284 for evidence.	209.251.180.146
TCP Sequence Number Approximation Vulnerability	Severe	False Positive	jayel on 2010-02-24	See case 32284 for evidence.	209.251.180.146
TCP Sequence Number Approximation Vulnerability	Severe	False Positive	jjames on 2010-04-30	See case 33676	209.251.180.146
TCP Sequence Number Approximation Vulnerability	Severe	False Positive	efagone on 2010-03-01	see case 32423	209.251.180.146
TCP Sequence Number Approximation Vulnerability	Severe	False Positive	efagone on 2010-03-03	see case 32471	209.251.180.146
TCP Sequence Number Approximation Vulnerability	Severe	False Positive	efagone on 2010-03-03	see case 32471	209.251.180.146
TCP Sequence Number	Severe	False	efagone on 2010-03-03	see case 32471	209.251.180.146

PCI Audit Report

Vulnerability	Severity	Reason	Authorization	Comments	Affects
Approximation Vulnerability		Positive			
TCP Sequence Number Approximation Vulnerability	Severe	False Positive	efagone on 2010-03-03	see case 32471	209.251.180.146
TCP Sequence Number Approximation Vulnerability	Severe	False Positive	efagone on 2010-03-03	see case 32471	209.251.180.146
TCP Sequence Number Approximation Vulnerability	Severe	False Positive	efagone on 2010-03-09	see case 32471	209.251.180.146
TCP Sequence Number Approximation Vulnerability	Severe	False Positive	efagone on 2010-03-09	see case 32471	209.251.180.146
TCP Sequence Number Approximation Vulnerability	Severe	False Positive	efagone on 2010-03-09	see case 32471	209.251.180.146
ASP.NET debug feature enabled	Severe	False Positive	jjames on 2010-05-03	see case 33676	209.251.180.146
Untrusted TLS/SSL server X.509 certificate	Severe	False Positive	jjames on 2010-04-30	see case 33676	209.251.180.146
MS08-020: Vulnerability in DNS Client Could Allow Spoofing (945553)	Severe	False Positive	cbun on 2010-02-09	Case 31717.	209.251.180.146
MS08-020: Vulnerability in DNS Client Could Allow Spoofing (945553)	Severe	False Positive	atu on 2009-12-22	See Case 31428	209.251.180.146
MS08-020: Vulnerability in DNS Client Could Allow Spoofing (945553)	Severe	False Positive	jjames on 2010-04-30	see case 33676	209.251.180.146
Apache ETag Inode Information Leakage	Moderate	False Positive	jjames on 2010-05-03	see case 33676	209.251.180.146
WebDAV Extensions are Enabled	Moderate	False Positive	jjames on 2010-05-03	see case 33676	209.251.180.146