The following information is a sample of technical data presented to a customer after a vulnerability assessment. The data have been redacted and some standard sections removed entirely to protect client confidentiality

Table of Contents

Vulnerabilities Identified

212 Total Vulnerabilities Identified Summary

[redacted] **Results:**

1. Does not use SSL/TLS.
    - Contains web mail login over HTTP, HTTP is insecure for credentials.
    - Vulnerable to Man-In-The-Middle attacks
2. Has files in web root which allow fingerprinting
3. Has the "X-Powered-By", "X-Generator", and "Server" headers set.
    - This allows an attacker to effectively fingerprint server software versions and operating systems.

Recommendations f[redacted]:

1. Upgrade server to use TLS.
2. Remove these extraneous files from web root.
3. Do not return these headers in the HTTP response. Configure web server to not output these headers.
4. Upgrade to Drupal 7.44.

speedtest[redacted] Results:

1. Does not use SSL/TLS.
    - Vulnerable to MITM attacks.
2. Using VSFTPD 3.0.2, which has 1 known vulnerability
3. Using OpenSSH 6.6.1, which has 3 known vulnerabilities:
4. Has SSH on Port 22 publicly exposed
5. Using weak MAC algorithms, such as MD5 and potentially SHA1.

Recommendations for speedt[redacted]n:

1. Upgrade server to use TLS.
2. Upgrade VSFTPD to version 3.0.3
3. Upgrade to OpenSSH 7.2p2
4. Consider restricting access to only machines / networks that need access.
5. Disable weak MAC algorithms.

webmail[redacted]net Results:

1. uses a version of jQuery with known vulnerabilities (1.4.2)
2. 404 page returns Apache version and operating system details.
3. Has "X-Powered-By" and "Server" headers with version which allow for easy fingerprinting.

Recommendation:

1. Updated SquirrelMail
2. Modify Web Server configuration to not display these details.
3. Modify web server configuration to not output these headers.

1 Scan Results

1.1 Identified Hosts

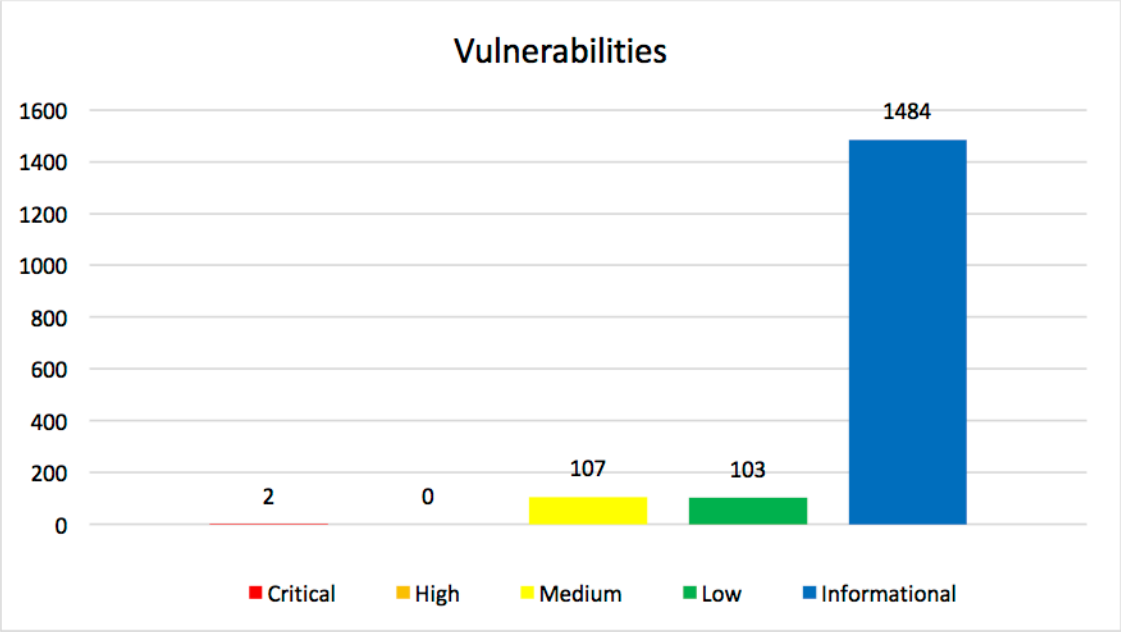
The hosts identified during this vulnerability scan is presented in the table below.

Host Name	IP
adm	167
adm	167
ann	108
aut	216
con	108
e-sc	64.
ebil	216
ema	216
esu	64.
f1pl	167
f2pl	167
ftp.	167
isol	167
mai	64.
msc	216
my.	167
myp	108
owa	216
patr	216
patr	216
pws	167
red.	216
smt	216
spa	208
spe	67.
spe	67.
spe	67.
spe	67.
spe	67.
sste	216
sup	64.
teln	167
voip	108
vpn	167
vpn	167
web	64.
ww	167
ww	64.

1.2 Vulnerabilities

1.2.1 Vulnerability Summary

The bar graph below displays the distribution of Vulnerabilities found by ProCircular, during this vulnerability scan.



1.2.2 Host Overview

The table below displays the number of vulnerabilities identified for each host, during this vulnerability scan.

IP	Informational	Low	Medium	High	Critical
64	441	51	12	0	0
67	165	15	10	0	0
10	42	0	2	0	0
10	47	1	3	0	0
10	48	1	3	0	0
10	13	0	0	0	0
16	32	0	6	0	0
16	26	1	1	0	0
16	39	1	5	0	1
16	32	0	3	0	1
16	24	2	0	0	0
16	29	0	3	0	0
16	29	0	2	0	0
16	52	6	16	0	0
16	52	6	16	0	0
16	23	0	1	0	0
20	70	4	4	0	0
21	31	5	0	0	0
21	9	0	0	0	0
21	29	1	0	0	0
21	106	4	5	0	0
21	88	2	4	0	0
21	57	3	11	0	0

1.2.3 Vulnerabilities and Affected Hosts

All vulnerabilities identified by ProCircular, are presented below. Information about each vulnerability is presented together with the vulnerable hosts. The vulnerabilities are sorted by severity, with the most severe vulnerabilities first.

Synopsis	**The operating system running on the remote host is no longer supported.**
Ports	0
Severity	Critical
Risk	Critical
Description	According to its self-reported version number, the Unix operating system running on the remote host is no longer supported. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.
Solution	Upgrade to a version of the Unix operating system that is currently supported.
CVE numbers	
Affected IP addresses	

Synopsis	**Debugging functions are enabled on the remote web server.**
Ports	443,80
Severity	Medium
Risk	Medium
Description	The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.
Solution	Disable these methods. Refer to the plugin output for more information.
CVE numbers	CVE-2003-1567 CVE-2004-2320 CVE-2010-0386
Affected IP addresses	

Synopsis	The remote SSH server is configured to allow weak encryption algorithms or no algorithm at all.
Ports	22
Severity	Medium
Risk	Medium
Description	Nessus has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys.
Solution	Contact the vendor or consult product documentation to remove the weak ciphers.
CVE numbers	
Affected IP addresses	

Synopsis	The remote service encrypts traffic using a protocol with known weaknesses.
Ports	443,587,110,143
Severity	Medium
Risk	Medium
Description	The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws. An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients. NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC'S definition of 'strong cryptography'.
Solution	Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.1 (with approved cipher suites) or higher instead.
CVE numbers	
Affected IP addresses	

Synopsis	It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.
Ports	443
Severity	Medium
Risk	Medium
Description	The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode. MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections. As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service. The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism. This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability.
Solution	Disable SSLv3. Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.
CVE numbers	CVE-2014-3566
Affected IP addresses	

Synopsis	The remote IKEv1 service supports Aggressive Mode with Pre-Shared key.
Ports	500
Severity	Medium
Risk	Medium
Description	The remote Internet Key Exchange (IKE) version 1 service seems to support Aggressive Mode with Pre-Shared key (PSK) authentication. Such a configuration could allow an attacker to capture and crack the PSK of a VPN gateway and gain unauthorized access to private networks.
Solution	- Disable Aggressive Mode if supported. - Do not use Pre-Shared key for authentication if it's possible. - If using Pre-Shared key cannot be avoided, use very strong keys. - If possible, do not allow VPN connections from any IP addresses. Note that this plugin does not run over IPv6.
CVE numbers	CVE-2002-1623
Affected IP addresses	

Synopsis	The remote web server contains a web application that uses a Java framework that is affected by a security bypass vulnerability.
Ports	8080,80
Severity	Medium
Risk	Medium
Description	The remote web application appears to use Struts 2, a web framework that utilizes OGNL (Object-Graph Navigation Language) as an expression language. The version of Struts 2 in use is affected by a security bypass vulnerability due to the application allowing manipulation of the ClassLoader via the 'class' parameter, which is directly mapped to the getClass() method. A remote, unauthenticated attacker can take advantage of this issue to manipulate the ClassLoader used by the application server, allowing for the bypass of certain security restrictions. Note that this plugin will only report the first vulnerable instance of a Struts 2 application. Note also that the application may also be affected by a denial of service vulnerability; however, Nessus has not tested for this additional issue.
Solution	Upgrade to version 2.3.16.1 or later.
CVE numbers	CVE-2014-0094
Affected IP addresses	[redacted]

Synopsis	The remote web server may fail to mitigate a class of web application vulnerabilities.
Ports	8080,80,443
Severity	Medium
Risk	Medium
Description	The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions. X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors. Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource. Note that while the X-Frame-Options and Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g., frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions.
Solution	Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response. This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.
CVE numbers	
Affected IP addresses	[redacted]

Synopsis	The remote web server is prone to cross-site scripting attacks.
Ports	80
Severity	Medium
Risk	Medium
Description	The remote web server hosts CGI scripts that fail to adequately sanitize request strings of malicious JavaScript. By leveraging this issue, an attacker may be able to cause arbitrary HTML and script code to be executed in a user's browser within the security context of the affected site. These XSS are likely to be 'non-persistent' or 'reflected'.
Solution	Restrict access to the vulnerable application. Contact the vendor for a patch or upgrade.
CVE numbers	
Affected IP addresses	[redacted]

Synopsis	The remote web server is affected by an information disclosure vulnerability.
Ports	80
Severity	Medium
Risk	Medium
Description	The remote web server is affected by an information disclosure vulnerability due to the ETag header providing sensitive information that could aid an attacker, such as the inode number of requested files.
Solution	Modify the HTTP ETag header of the web server to not include file inodes in the ETag header calculation. Refer to the linked Apache documentation for more information.
CVE numbers	CVE-2003-1418
Affected IP addresses	

Synopsis	The remote service allows insecure renegotiation of TLS / SSL connections.
Ports	587,110,143,443
Severity	Medium
Risk	Medium
Description	The remote service encrypts traffic using TLS / SSL but allows a client to insecurely renegotiate the connection after the initial handshake. An unauthenticated, remote attacker may be able to leverage this issue to inject an arbitrary amount of plaintext into the beginning of the application protocol stream, which could facilitate man-in-the-middle attacks if the service assumes that the sessions before and after renegotiation are from the same 'client' and merges them at the application layer.
Solution	Contact the vendor for specific patch information.
CVE numbers	CVE-2009-3555
Affected IP addresses	

Synopsis	An SSL certificate in the certificate chain has been signed using a weak hash algorithm.
Ports	587,110,143,443
Severity	Medium
Risk	Medium
Description	The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service. Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm. Note that certificates in the chain that are contained in the Nessus CA database have been ignored.
Solution	Contact the Certificate Authority to have the certificate reissued.
CVE numbers	CVE-2004-2761
Affected IP addresses	[redacted]

Synopsis	The SSL certificate for this service cannot be trusted.
Ports	587,110,143,443
Severity	Medium
Risk	Medium
Description	The server's X.509 certificate does not have a signature from a known public certificate authority. This situation can occur in three different ways, each of which results in a break in the chain below which certificates cannot be trusted. First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority. Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates. Third, the certificate chain may contain a signature that either didn't match the certificate's information, or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize. If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.
Solution	Purchase or generate a proper certificate for this service.
CVE numbers	
Affected IP addresses	[redacted]

Synopsis	The remote server's SSL certificate has already expired.
Ports	443
Severity	Medium
Risk	Medium
Description	This plugin checks expiry dates of certificates associated with SSL- enabled services on the target and reports whether any have already expired.
Solution	Purchase or generate a new SSL certificate to replace the existing one.
CVE numbers	
Affected IP addresses	

Synopsis	Confidential data may be disclosed on this server.
Ports	80
Severity	Medium
Risk	Medium
Description	The remote web server hosts CGI scripts that fail to adequately sanitize request strings. By leveraging this issue, an attacker may be able to include a local file and disclose its content.
Solution	Restrict access to the vulnerable application. Contact the vendor for a patch or upgrade.
CVE numbers	
Affected IP addresses	

Synopsis	The remote mail server is affected by an information disclosure vulnerability.
Ports	443
Severity	Medium
Risk	Medium
Description	The Microsoft Exchange Client Access Server (CAS) is affected by an information disclosure vulnerability. A remote, unauthenticated attacker can exploit this vulnerability to learn the server's internal IP address.
Solution	There is no known fix at this time.
CVE numbers	
Affected IP addresses	

Synopsis	The configuration of PHP on the remote host allows disclosure of sensitive information.
Ports	80,443
Severity	Medium
Risk	Medium
Description	The PHP install on the remote server is configured in a way that allows disclosure of potentially sensitive information to an attacker through a special URL. Such a URL triggers an Easter egg built into PHP itself. Other such Easter eggs likely exist, but Nessus has not checked for them.
Solution	In the PHP configuration file, php.ini, set the value for 'expose_php' to 'Off' to disable this behavior. Restart the web server daemon to put this change into effect.
CVE numbers	
Affected IP addresses	[redacted]

Synopsis	The remote web server contains example files.
Ports	443,80
Severity	Medium
Risk	Medium
Description	Example JSPs and Servlets are installed in the remote Apache Tomcat servlet / JSP container. These files should be removed as they may help an attacker uncover information about the remote Tomcat install or host itself. The example files may also contain vulnerabilities such as cross-site scripting vulnerabilities.
Solution	Review the files and delete those that are not needed.
CVE numbers	
Affected IP addresses	[redacted]

Synopsis	The remote Apache Tomcat server is affected by an information disclosure vulnerability.
Ports	443,80
Severity	Medium
Risk	Medium
Description	The remote Apache Tomcat web server is affected by an information disclosure vulnerability in the index page of the Manager and Host Manager applications. An unauthenticated, remote attacker can exploit this vulnerability to obtain a valid cross-site request forgery (XSRF) token during the redirect issued when requesting /manager/ or /host-manager/. This token can be utilized by an attacker to construct an XSRF attack. Note that there are reportedly several additional vulnerabilities; however, Nessus has not tested for these.
Solution	Upgrade to Apache Tomcat version 7.0.68 / 8.0.32 / 9.0.0.M3 or later.
CVE numbers	CVE-2015-5351
Affected IP addresses	[redacted]

Synopsis	The remote service supports the use of weak SSL ciphers.
Ports	443
Severity	Medium
Risk	Medium
Description	The remote host supports the use of SSL ciphers that offer weak encryption. Note: This is considerably easier to exploit if the attacker is on the same physical network.
Solution	Reconfigure the affected application, if possible to avoid the use of weak ciphers.
CVE numbers	
Affected IP addresses	

Synopsis	The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits.
Ports	995,993,443
Severity	Low
Risk	Low
Description	The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections.
Solution	Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.
CVE numbers	CVE-2015-4000
Affected IP addresses	

Synopsis	The remote POP3 daemon allows credentials to be transmitted in cleartext.
Ports	110
Severity	Low
Risk	Low
Description	The remote host is running a POP3 daemon that allows cleartext logins over unencrypted connections. An attacker can uncover user names and passwords by sniffing traffic to the POP3 daemon if a less secure authentication mechanism (eg, USER command, AUTH PLAIN, AUTH LOGIN) is used.
Solution	Contact your vendor for a fix or encrypt traffic with SSL / TLS using stunnel.
CVE numbers	
Affected IP addresses	

Synopsis	Authentication credentials might be intercepted.
Ports	21
Severity	Low
Risk	Low
Description	The remote FTP server allows the user's name and password to be transmitted in cleartext, which could be intercepted by a network sniffer or a man-in-the-middle attack.
Solution	Switch to SFTP (part of the SSH suite) or FTPS (FTP over SSL/TLS). In the latter case, configure the server so that control connections are encrypted.
CVE numbers	
Affected IP addresses	[redacted]

Synopsis	The remote service supports the use of the RC4 cipher.
Ports	110,143,443,995,993,8443,587,465
Severity	Low
Risk	Low
Description	The remote host supports the use of RC4 in one or more cipher suites. The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness. If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.
Solution	Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.
CVE numbers	CVE-2013-2566 CVE-2015-2808
Affected IP addresses	[redacted]

Synopsis	The SSH server is configured to use Cipher Block Chaining.
Ports	22
Severity	Low
Risk	Low
Description	The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext. Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.
Solution	Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.
CVE numbers	CVE-2008-5161
Affected IP addresses	[redacted]

Synopsis	The remote SSH server is configured to allow MD5 and 96-bit MAC algorithms.
Ports	22
Severity	Low
Risk	Low
Description	The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak. Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.
Solution	Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.
CVE numbers	
Affected IP addresses	

Synopsis	The remote web server might transmit credentials in cleartext.
Ports	8080,80
Severity	Low
Risk	Low
Description	The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext. An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users.
Solution	Make sure that every sensitive form transmits content over HTTPS.
CVE numbers	
Affected IP addresses	

Synopsis	The remote mail server allows cleartext logins.
Ports	587
Severity	Low
Risk	Low
Description	The remote host is running an SMTP server that advertises that it allows cleartext logins over unencrypted connections. An attacker may be able to uncover user names and passwords by sniffing traffic to the server if a less secure authentication mechanism (i.e. LOGIN or PLAIN) is used.
Solution	Configure the service to support less secure authentication mechanisms only over an encrypted channel.
CVE numbers	
Affected IP addresses	

Synopsis	The remote service supports the use of anonymous SSL ciphers.
Ports	587,465
Severity	Low
Risk	Low
Description	The remote host supports the use of anonymous SSL ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack. Note: This is considerably easier to exploit if the attacker is on the same physical network.
Solution	Reconfigure the affected application if possible to avoid use of weak ciphers.
CVE numbers	CVE-2007-1858
Affected IP addresses	

Synopsis	This web server leaks a private IP address through its HTTP headers.
Ports	443
Severity	Low
Risk	Low
Description	This may expose internal IP addresses that are usually hidden or masked behind a Network Address Translation (NAT) Firewall or proxy server. There is a known issue with Microsoft IIS 4.0 doing this in its default configuration. This may also affect other web servers, web applications, web proxies, load balancers and through a variety of misconfigurations related to redirection.
Solution	None
CVE numbers	CVE-2000-0649
Affected IP addresses	

Synopsis	The remote web server seems to transmit credentials in cleartext.
Ports	80
Severity	Low
Risk	Low
Description	The remote web server contains web pages that are protected by 'Basic' authentication over cleartext. An attacker eavesdropping the traffic might obtain logins and passwords of valid users.
Solution	Make sure that HTTP authentication is transmitted over HTTPS.
CVE numbers	
Affected IP addresses	

Synopsis	It was possible to obtain sensitive information from the remote host with TLS-enabled services.
Ports	443
Severity	Low
Risk	Low
Description	The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability due to an error in the implementation of ciphersuites that use AES in CBC mode with HMAC-SHA1 or HMAC-SHA256. The implementation is specially written to use the AES acceleration available in x86/amd64 processors (AES-NI). The error messages returned by the server allow allow a man-in-the-middle attacker to conduct a padding oracle attack, resulting in the ability to decrypt network traffic.
Solution	Upgrade to OpenSSL version 1.0.1t / 1.0.2h or later.
CVE numbers	CVE-2016-2107
Affected IP addresses	

Synopsis	A DNS server is listening on the remote host.
Ports	53
Severity	Informational
Risk	None
Description	The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.
Solution	Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.
CVE numbers	
Affected IP addresses	

Synopsis	The remote mail service supports encrypting traffic.
Ports	110
Severity	Informational
Risk	None
Description	The remote POP3 service supports the use of the 'STLS' command to switch from a cleartext to an encrypted communications channel.
Solution	n/a
CVE numbers	
Affected IP addresses	

Synopsis	The remote mail service supports encrypting traffic.
Ports	143
Severity	Informational
Risk	None
Description	The remote IMAP service supports the use of the 'STARTTLS' command to switch from a cleartext to an encrypted communications channel.
Solution	n/a
CVE numbers	
Affected IP addresses	

Synopsis	The name of the Linux distribution running on the remote host was found in the banner of the web server.
Ports	0
Severity	Informational
Risk	None
Description	This plugin extracts the banner of the Apache web server and attempts to determine which Linux distribution the remote host is running.
Solution	If you do not wish to display this information, edit 'httpd.conf' and set the directive 'ServerTokens Prod' and restart Apache. n/a
CVE numbers	
Affected IP addresses	

Synopsis	Some information about the remote HTTP configuration can be extracted.
Ports	443,80,8443,8080,9000,8089
Severity	Informational
Risk	None
Description	This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc... This test is informational only and does not denote any security problem.
Solution	n/a
CVE numbers	
Affected IP addresses	

Synopsis	The remote web server is not enforcing HSTS.
Ports	443,8443
Severity	Informational
Risk	None
Description	The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.
Solution	Configure the remote web server to use HSTS.
CVE numbers	
Affected IP addresses	

Synopsis	This plugin determines which HTTP methods are allowed on various CGI directories.
Ports	443,80,8443,8080,9000,8089
Severity	Informational
Risk	None
Description	By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory. As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes' in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501. Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.
Solution	n/a
CVE numbers	
Affected IP addresses	

Synopsis	A web server is running on the remote host.
Ports	443,80,9000,8089
Severity	Informational
Risk	None
Description	This plugin attempts to determine the type and the version of the remote web server.
Solution	n/a
CVE numbers	
Affected IP addresses	

Synopsis	The remote service requests an SSL client certificate.
Ports	110,143
Severity	Informational
Risk	None
Description	The remote service encrypts communications using SSL/TLS, requests a client certificate, and may require a valid certificate in order to establish a connection to the underlying service.
Solution	n/a
CVE numbers	
Affected IP addresses	

Synopsis	The remote service appears to use OpenSSL to encrypt traffic.
Ports	110,143,443,995,993,587,465
Severity	Informational
Risk	None
Description	Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic. Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).
Solution	n/a
CVE numbers	
Affected IP addresses	

Synopsis	An IMAP server is running on the remote host.
Ports	993,143
Severity	Informational
Risk	None
Description	An IMAP (Internet Message Access Protocol) server is installed and running on the remote host.
Solution	n/a
CVE numbers	
Affected IP addresses	

Synopsis	A POP server is listening on the remote port.
Ports	995,110
Severity	Informational
Risk	None
Description	The remote host is running a server that understands the Post Office Protocol (POP), used by email clients to retrieve messages from a server, possibly across a network link.
Solution	Disable this service if you do not use it.
CVE numbers	
Affected IP addresses	

Synopsis	An FTP server is listening on a remote port.
Ports	21
Severity	Informational
Risk	None
Description	It is possible to obtain the banner of the remote FTP server by connecting to a remote port.
Solution	n/a
CVE numbers	
Affected IP addresses	

Synopsis	The remote service could be identified.
Ports	995,993,443,143,110,80,21,22,8443,8080,587,465,9000,8089
Severity	Informational
Risk	None
Description	Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.
Solution	n/a
CVE numbers	
Affected IP addresses	

Synopsis	This plugin displays information about the Nessus scan.
Ports	0
Severity	Informational
Risk	None
Description	This plugin displays, for each tested host, information about the scan itself : - The version of the plugin set. - The type of scanner (Nessus or Nessus Home). - The version of the Nessus Engine. - The port scanner(s) used. - The port range scanned. - Whether credentialed or third-party patch management checks are possible. - The date of the scan. - The duration of the scan. - The number of hosts scanned in parallel. - The number of checks done in parallel.
Solution	n/a
CVE numbers	
Affected IP addresses	

Synopsis	Previously open ports are now closed.
Ports	0
Severity	Informational
Risk	None
	One of several ports that were previously open are now closed or unresponsive. There are several possible reasons for this : - The scan may have caused a service to freeze or stop running. - An administrator may have stopped a particular service during the scanning process. This might be an availability problem related to the following : - A network outage has been experienced during the scan, and the remote network cannot be reached anymore by the scanner. - This scanner may has been blacklisted by the system administrator or by an automatic intrusion detection / prevention system that detected the scan. - The remote host is now down, either because a user turned it off during the scan or because a select denial of service was effective. In any case, the audit of the remote host might be incomplete and may need to be done again.
Solution	- Increase checks_read_timeout and/or reduce max_checks. - Disable any IPS during the Nessus scan
CVE numbers	
Affected IP addresses	

Synopsis	Security patches are backported.
Ports	21
Severity	Informational
Risk	None
Description	Security patches may have been 'backported' to the remote FTP server without changing its version number. Banner-based checks have been disabled to avoid false positives. Note that this test is informational only and does not denote any security problem.
Solution	n/a
CVE numbers	
Affected IP addresses	

Synopsis	Security patches are backported.
Ports	443,80
Severity	Informational
Risk	None
Description	Security patches may have been 'backported' to the remote HTTP server without changing its version number. Banner-based checks have been disabled to avoid false positives. Note that this test is informational only and does not denote any security problem.
Solution	n/a
CVE numbers	
Affected IP addresses	

Synopsis	The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.
Ports	110,143,443,995,993,8443,587,465
Severity	Informational
Risk	None
Description	The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.
Solution	n/a
CVE numbers	
Affected IP addresses	

Synopsis	The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.
Ports	110,143,443,995,993,8443,587,465
Severity	Informational
Risk	None
Description	The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.
Solution	n/a
CVE numbers	
Affected IP addresses	

Synopsis	The remote service encrypts communications using SSL.
Ports	110,143,443,995,993,8443,587,465
Severity	Informational
Risk	None
Description	This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.
Solution	n/a
CVE numbers	
Affected IP addresses	

Synopsis	It is possible to enumerate CPE names that matched on the remote system.
Ports	0
Severity	Informational
Risk	None
Description	By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host. Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.
Solution	n/a
CVE numbers	
Affected IP addresses	

Synopsis	It is possible to guess the remote device type.
Ports	0
Severity	Informational
Risk	None
Description	Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).
Solution	n/a
CVE numbers	
Affected IP addresses	

Synopsis	It is possible to guess the remote operating system.
Ports	0
Severity	Informational
Risk	None
Description	Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.
Solution	n/a
CVE numbers	
Affected IP addresses	

Synopsis	Nessus has detected potential virtual hosts.
Ports	0
Severity	Informational
Risk	None
Description	Hostnames different from the current hostname have been collected by miscellaneous plugins. Nessus has generated a list of hostnames that point to the remote host. Note that these are only the alternate hostnames for vhosts discovered on a web server. Different web servers may be hosted on name-based virtual hosts.
Solution	If you want to test them, re-scan using the special vhost syntax, such as : www.example.com[192.0.32.10]
CVE numbers	
Affected IP addresses	

Synopsis	This plugin displays the SSL certificate.
Ports	110,143,443,995,993,8443,587,465
Severity	Informational
Risk	None
Description	This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.
Solution	n/a
CVE numbers	
Affected IP addresses	

Synopsis	The remote service encrypts communications.
Ports	110,143,443,995,993,8443,587,465
Severity	Informational
Risk	None
Description	This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.
Solution	n/a
CVE numbers	
Affected IP addresses	

Synopsis	The remote service implements TCP timestamps.
Ports	0
Severity	Informational
Risk	None
Description	The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.
Solution	n/a
CVE numbers	
Affected IP addresses	

Synopsis	It was possible to resolve the name of the remote host.
Ports	0
Severity	Informational
Risk	None
Description	Nessus was able to resolve the FQDN of the remote host.
Solution	n/a
CVE numbers	
Affected IP addresses	

Synopsis	It was possible to obtain traceroute information.
Ports	0
Severity	Informational
Risk	None
Description	Makes a traceroute to the remote host.
Solution	n/a
CVE numbers	
Affected IP addresses	

Synopsis	It is possible to determine which TCP ports are open.
Ports	995,110,993,21,53,80,443,143,22,8443,8080,587,465,5060,9000,1935,8089
Severity	Informational
Risk	None
Description	This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.
Solution	Protect your target with an IP filter.
CVE numbers	
Affected IP addresses	

Synopsis	It was possible to identify the status of the remote host (alive or dead)
Ports	0
Severity	Informational
Risk	None
Description	This plugin attempts to determine if the remote host is alive using one or more ping types : - An ARP ping, provided the host is on the local subnet and Nessus is running over ethernet. - An ICMP ping. - A TCP ping, in which the plugin sends to the remote host a packet with the flag SYN, and the host will reply with a RST or a SYN/ACK. - A UDP ping (DNS, RPC, NTP, etc).
Solution	n/a
CVE numbers	
Affected IP addresses	

Synopsis	An SSH server is listening on this port.
Ports	22
Severity	Informational
Risk	None
Description	This script detects which algorithms and languages are supported by the remote service for encrypting communications.
Solution	n/a
CVE numbers	
Affected IP addresses	

Synopsis	An FTP server is listening on the remote port.
Ports	21
Severity	Informational
Risk	None
Description	The remote host is running vsftpd, an FTP server for UNIX-like systems written in C.
Solution	n/a
CVE numbers	
Affected IP addresses	

Synopsis	The remote web server contains a 'crossdomain.xml' file.
Ports	80
Severity	Informational
Risk	None
Description	The remote web server contains a cross-domain policy file. This is a simple XML file used by Adobe's Flash Player to allow access to data that resides outside the exact web domain from which a Flash movie file originated.
Solution	Review the contents of the policy file carefully. Improper policies, especially an unrestricted one with just '*', could allow for cross- site request forgery and cross-site scripting attacks against the web server.
CVE numbers	
Affected IP addresses	

Synopsis	The remote web server does not take steps to mitigate a class of web application vulnerabilities.
Ports	80,8080,443
Severity	Informational
Risk	None
Description	The remote web server in some responses sets a permissive X-Frame-Options response header or does not set one at all. The X-Frame-Options header has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors
Solution	Set a properly configured X-Frame-Options header for all requested resources.
CVE numbers	
Affected IP addresses	

Synopsis	The remote web server does not take steps to mitigate a class of web application vulnerabilities.
Ports	80,8080,443
Severity	Informational
Risk	None
Description	The remote web server in some responses sets a permissive Content-Security-Policy (CSP) response header or does not set one at all. The CSP header has been proposed by the W3C Web Application Security Working Group as a way to mitigate cross-site scripting and clickjacking attacks.
Solution	Set a properly configured Content-Security-Policy header for all requested resources.
CVE numbers	
Affected IP addresses	

Synopsis	Security patches have been backported.
Ports	80,443
Severity	Informational
Risk	None
Description	Security patches may have been 'backported' to the remote PHP install without changing its version number. Banner-based checks have been disabled to avoid false positives. Note that this test is informational only and does not denote any security problem.
Solution	n/a
CVE numbers	
Affected IP addresses	

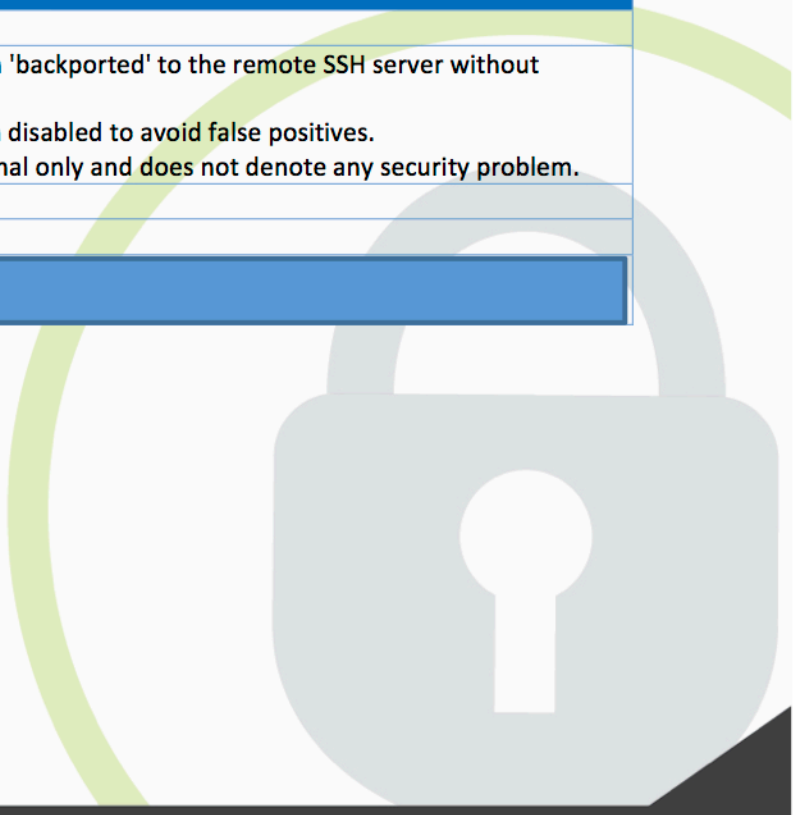
Synopsis	It is possible to obtain the version number of the remote PHP install.
Ports	80,443
Severity	Informational
Risk	None
Description	This plugin attempts to determine the version of PHP available on the remote web server.
Solution	n/a
CVE numbers	
Affected IP addresses	

Synopsis	The remote web server hosts linkable content that can be crawled by Nessus.
Ports	80,8080,443
Severity	Informational
Risk	None
Description	The remote web server contains linkable content that can be used to gather information about a target.
Solution	n/a
CVE numbers	
Affected IP addresses	

Synopsis	It is possible to enumerate directories on the web server.
Ports	80,8080,443
Severity	Informational
Risk	None
Description	This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.
Solution	n/a
CVE numbers	
Affected IP addresses	

Synopsis	An SSH server is listening on this port.
Ports	22
Severity	Informational
Risk	None
Description	It is possible to obtain information about the remote SSH server by sending an empty authentication request.
Solution	n/a
CVE numbers	
Affected IP addresses	

Synopsis	Security patches are backported.
Ports	22
Severity	Informational
Risk	None
Description	Security patches may have been 'backported' to the remote SSH server without changing its version number. Banner-based checks have been disabled to avoid false positives. Note that this test is informational only and does not denote any security problem.
Solution	n/a
CVE numbers	
Affected IP addresses	



Synopsis	A SSH server is running on the remote host.
Ports	22
Severity	Informational
Risk	None
Description	This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.
Solution	n/a
CVE numbers	
Affected IP addresses	

Synopsis	It is possible to determine the exact time set on the remote host.
Ports	0
Severity	Informational
Risk	None
Description	The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols. Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.
Solution	Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).
CVE numbers	CVE-1999-0524
Affected IP addresses	

Synopsis	The remote host is an SSL VPN server.
Ports	443
Severity	Informational
Risk	None
Description	The remote host is a Cisco Adaptive Security Appliance (ASA) running an SSL VPN server.
Solution	n/a
CVE numbers	
Affected IP addresses	

Synopsis	A VPN server is listening on the remote port.
Ports	500
Severity	Informational
Risk	None
Description	The remote host seems to be enabled to do Internet Key Exchange (IKE) version 1. This is typically indicative of a VPN server. VPN servers are used to connect remote hosts into internal resources. Make sure that the use of this VPN endpoint is done in accordance with your corporate security policy. Note that if the remote host is not configured to allow the Nessus host to perform IKE/IPSEC negotiations, Nessus won't be able to detect the IKE service. Also note that this plugin does not run over IPv6.
Solution	If this service is not needed, disable it or filter incoming traffic to this port.
CVE numbers	
Affected IP addresses	

Synopsis	The remote host allows resuming SSL sessions.
Ports	443,587,110,143
Severity	Informational
Risk	None
Description	This script detects whether a host allows resuming SSL sessions by performing a full SSL handshake to receive a session ID, and then reconnecting with the previously used session ID. If the server accepts the session ID in the second connection, the server maintains a cache of sessions that can be resumed.
Solution	n/a
CVE numbers	
Affected IP addresses	

Synopsis	Some generic CGI attacks ran out of time.
Ports	8080,80,443
Severity	Informational
Risk	None
Description	Some generic CGI tests ran out of time during the scan. The results may be incomplete.
Solution	Consider increasing the 'maximum run time (min)' preference for the 'Web Application Tests Settings' in order to prevent the CGI scanning from timing out. Less ambitious options could also be used, such as : - Combinations of arguments values = 'all combinations' is much slower than 'two pairs' or 'single'. - Stop at first flaw = 'per port' is quicker. - In 'some pairs' or 'some combinations' mode, try reducing web_app_tests.tested_values_for_each_parameter in nessusd.conf
CVE numbers	
Affected IP addresses	

Synopsis	Load estimation for web application tests.
Ports	8080,80,443
Severity	Informational
Risk	None
Description	This script computes the maximum number of requests that would be done by the generic web tests, depending on miscellaneous options. It does not perform any test by itself. The results can be used to estimate the duration of these tests, or the complexity of additional manual tests. Note that the script does not try to compute this duration based on external factors such as the network and web servers loads.
Solution	n/a
CVE numbers	
Affected IP addresses	

Synopsis	An application was found that may use CGI parameters to control sensitive information.
Ports	8080,80,443
Severity	Informational
Risk	None
Description	According to their names, some CGI parameters may control sensitive data (e.g., ID, privileges, commands, prices, credit card data, etc.). In the course of using an application, these variables may disclose sensitive data or be prone to tampering that could result in privilege escalation. These parameters should be examined to determine what type of data is controlled and if it poses a security risk. ** This plugin only reports information that may be useful for auditors ** or pen-testers, not a real flaw.
Solution	Ensure sensitive data is not disclosed by CGI parameters. In addition, do not use CGI parameters to control access to resources or privileges.
CVE numbers	
Affected IP addresses	

Synopsis	The remote web server redirects requests to the root directory.
Ports	8443,8080,443,80
Severity	Informational
Risk	None
Description	The remote web server issues an HTTP redirect when requesting the root directory of the web server. This plugin is informational only and does not denote a security problem.
Solution	Analyze the redirect(s) to verify that this is valid operation for your web server and/or application.
CVE numbers	
Affected IP addresses	

Synopsis	The remote web server does not return 404 error codes.
Ports	8443,8080,443,80
Severity	Informational
Risk	None
Description	The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page. Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.
Solution	n/a
CVE numbers	
Affected IP addresses	

Synopsis	The 'autocomplete' attribute is not disabled on password fields.
Ports	8080,80,443
Severity	Informational
Risk	None
Description	The remote web server contains at least one HTML form field that has an input of type 'password' where 'autocomplete' is not set to 'off'. While this does not represent a risk to this web server per se, it does mean that users who use the affected forms may have their credentials saved in their browsers, which could in turn lead to a loss of confidentiality if any of them use a shared host or if their machine is compromised at some point.
Solution	Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.
CVE numbers	
Affected IP addresses	

Synopsis	HTTP session cookies might be vulnerable to cross-site scripting attacks.
Ports	8443,8080,443,80,9000
Severity	Informational
Risk	None
Description	The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, one or more of those cookies are not marked 'HttpOnly', meaning that a malicious client-side script, such as JavaScript, could read them. The HttpOnly flag is a security mechanism to protect against cross-site scripting attacks, which was proposed by Microsoft and initially implemented in Internet Explorer. All modern browsers now support it. Note that this plugin detects all general cookies missing the HttpOnly cookie flag, whereas plugin 48432 (Web Application Session Cookies Not Marked HttpOnly) will only detect session cookies from an authenticated session missing the HttpOnly cookie flag.
Solution	Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision. If possible, add the 'HttpOnly' attribute to all session cookies and any cookies containing sensitive data.
CVE numbers	
Affected IP addresses	

Synopsis	HTTP session cookies might be transmitted in cleartext.
Ports	8443,8080,443,80,9000
Severity	Informational
Risk	None
Description	The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, there are instances where the application is running over unencrypted HTTP or the cookies are not marked 'secure', meaning the browser could send them back over an unencrypted link under certain circumstances. As a result, it may be possible for a remote attacker to intercept these cookies. Note that this plugin detects all general cookies missing the 'secure' cookie flag, whereas plugin 49218 (Web Application Session Cookies Not Marked Secure) will only detect session cookies from an authenticated session missing the secure cookie flag.
Solution	Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision. If possible, ensure all communication occurs over an encrypted channel and add the 'secure' attribute to all session cookies or any cookies containing sensitive data.
CVE numbers	
Affected IP addresses	

Synopsis	Nessus can crawl the remote website.
Ports	8080,80,443
Severity	Informational
Risk	None
Description	This plugin makes a mirror of the remote website(s) and extracts the list of CGIs that are used by the remote host. It is suggested that you change the number of pages to mirror in the 'Options' section of the client.
Solution	n/a
CVE numbers	
Affected IP addresses	

Synopsis	The remote host is missing several patches.
Ports	0
Severity	Informational
Risk	None
Description	The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.
Solution	Install the patches listed below.
CVE numbers	
Affected IP addresses	

Synopsis	The remote mail server supports authentication.
Ports	587,465
Severity	Informational
Risk	None
Description	The remote SMTP server advertises that it supports authentication.
Solution	Review the list of methods and whether they're available over an encrypted channel.
CVE numbers	
Affected IP addresses	

Synopsis	The remote mail service supports encrypting traffic.
Ports	587
Severity	Informational
Risk	None
Description	The remote SMTP service supports the use of the 'STARTTLS' command to switch from a cleartext to an encrypted communications channel.
Solution	n/a
CVE numbers	
Affected IP addresses	

Synopsis	An SMTP server is listening on the remote port.
Ports	587,465
Severity	Informational
Risk	None
Description	The remote host is running a mail (SMTP) server on this port. Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it.
Solution	Disable this service if you do not use it, or filter incoming traffic to this port.
CVE numbers	
Affected IP addresses	

Synopsis	Some CGIs are candidate for extended injection tests.
Ports	80,443
Severity	Informational
Risk	None
Description	Nessus was able to to inject innocuous strings into CGI parameters and read them back in the HTTP response. The affected parameters are candidates for extended injection tests like cross-site scripting attacks. This is not a weakness per se, the main purpose of this test is to speed up other scripts. The results may be useful for a human pen-tester.
Solution	n/a
CVE numbers	
Affected IP addresses	

Synopsis	Links to external sites were gathered.
Ports	80,443
Severity	Informational
Risk	None
Description	Nessus gathered HREF links to external sites by crawling the remote web server.
Solution	n/a
CVE numbers	
Affected IP addresses	

Synopsis	The remote host's hostname is not consistent with DNS information.
Ports	0
Severity	Informational
Risk	None
Description	The name of this machine either does not resolve or resolves to a different IP address. This may come from a badly configured reverse DNS or from a host file in use on the Nessus scanning host. As a result, URLs in plugin output may not be directly usable in a web browser and some web tests may be incomplete.
Solution	Fix the reverse DNS or host file.
CVE numbers	
Affected IP addresses	

Synopsis	It is possible to obtain the version number of the remote DNS server.
Ports	53
Severity	Informational
Risk	None
Description	The remote host is running BIND or another DNS server that reports its version number when it receives a special request for the text 'version.bind' in the domain 'chaos'. This version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.
Solution	It is possible to hide the version number of BIND by using the 'version' directive in the 'options' section in named.conf.
CVE numbers	
Affected IP addresses	

Synopsis	Nessus was able to obtain version information on the remote DNS server.
Ports	53
Severity	Informational
Risk	None
Description	Nessus was able to obtain version information by sending a special TXT record query to the remote host. Note that this version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.
Solution	n/a
CVE numbers	
Affected IP addresses	

Synopsis	The remote service could be identified.
Ports	143
Severity	Informational
Risk	None
Description	It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives a 'HELP' request.
Solution	n/a
CVE numbers	
Affected IP addresses	

Synopsis	Nessus encountered errors while running its generic CGI attacks.
Ports	80
Severity	Informational
Risk	None
Description	Nessus ran into trouble while running its generic CGI tests against the remote web server (for example, connection refused, timeout, etc). When this happens, Nessus aborts the current test and switches to the next CGI script on the same port or to another web server. Thus, test results may be incomplete.
Solution	Rescan with a longer network timeout or less parallelism for example, by changing the following options in the scan policy : - Network -> Network Receive Timeout (check_read_timeout) - Options -> Number of hosts in parallel (max_hosts) - Options -> Number of checks in parallel (max_checks)
CVE numbers	
Affected IP addresses	

Synopsis	The remote web server contains a content management system written in PHP.
Ports	80
Severity	Informational
Risk	None
Description	The remote host is running Drupal, an open source content management system written in PHP.
Solution	Make sure the use of this program is in accordance with your corporate security policy.
CVE numbers	
Affected IP addresses	

Synopsis	The remote web server contains a 'robots.txt' file.
Ports	80
Severity	Informational
Risk	None
Description	The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a website for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks.
Solution	Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.
CVE numbers	
Affected IP addresses	

Synopsis	Email addresses were harvested from the web server.
Ports	80,443
Severity	Informational
Risk	None
Description	Nessus harvested HREF mailto: links and extracted email addresses by crawling the remote web server.
Solution	n/a
CVE numbers	
Affected IP addresses	

Synopsis	The remote system is a SIP signaling device.
Ports	5060
Severity	Informational
Risk	None
Description	The remote system is running software that speaks the Session Initiation Protocol (SIP). SIP is a messaging protocol to initiate communication sessions between systems. It is a protocol used mostly in IP Telephony networks / systems to setup, control, and teardown sessions between two or more systems.
Solution	If possible, filter incoming connections to the port so that it is used only by trusted sources.
CVE numbers	
Affected IP addresses	

Synopsis	It is possible to extract the version of Microsoft Exchange Server installed on the remote host.
Ports	443
Severity	Informational
Risk	None
Description	Microsoft Exchange Server with Outlook Web Access (OWA) embeds the Exchange version number inside the default HTML web page. By requesting the default HTML page, Nessus was able to extract the Microsoft Exchange server version.
Solution	n/a
CVE numbers	
Affected IP addresses	

Synopsis	A Flash media server is listening on the remote host.
Ports	1935
Severity	Informational
Risk	None
Description	The remote service supports Real Time Messaging Protocol (RTMP), a proprietary protocol used by Flash Player for streaming real-time audio, video, and objects using a binary connection.
Solution	Limit incoming traffic to this port if desired.
CVE numbers	
Affected IP addresses	

Synopsis	The remote web server hosts office-related files.
Ports	443,80
Severity	Informational
Risk	None
Description	This plugin connects to the remote web server and attempts to find office-related files such as .doc, .ppt, .xls, .pdf etc.
Solution	Make sure that such files do not contain any confidential or otherwise sensitive information and that they are only accessible to those with valid credentials.
CVE numbers	
Affected IP addresses	

Synopsis	The remote web server contains a graphic image that is prone to information disclosure.
Ports	443,80
Severity	Informational
Risk	None
Description	The 'favicon.ico' file found on the remote web server belongs to a popular web server. This may be used to fingerprint the web server.
Solution	Remove the 'favicon.ico' file or create a custom one for your site.
CVE numbers	
Affected IP addresses	

Synopsis	The remote web server reports its version number on error pages.
Ports	443,80
Severity	Informational
Risk	None
Description	Apache Tomcat is running on the remote host and is reporting its version number on the default error pages. A remote attacker can exploit this information to mount further attacks.
Solution	Replace the default error pages with custom error pages to hide the version number. Refer to the Apache wiki or the Java Servlet Specification for more information.
CVE numbers	
Affected IP addresses	

Synopsis	The remote web server seems to transmit credentials using Basic Authentication.
Ports	443
Severity	Informational
Risk	None
Description	The remote web server contains web pages that are protected by 'Basic' authentication over HTTPS. While this is not in itself a security flaw, in some organizations, the use of 'Basic' authentication is discouraged as, depending on the underlying implementation, it may be vulnerable to account brute-forcing or may encourage Man-in-The-Middle (MiTM) attacks.
Solution	Make sure that the use of HTTP 'Basic' authentication is in line with your organization's security policy.
CVE numbers	
Affected IP addresses	

Synopsis	The remote web server is not configured or is improperly configured.
Ports	443,80
Severity	Informational
Risk	None
Description	The remote web server uses its default welcome page. Therefore, it's probable that this server is not used at all or is serving content that is meant to be hidden.
Solution	Disable this service if you do not use it.
CVE numbers	
Affected IP addresses	

Synopsis	The SSL certificate commonName does not match the host name.
Ports	443
Severity	Informational
Risk	None
Description	This service presents an SSL certificate for which the 'commonName' (CN) does not match the host name on which the service listens.
Solution	If the machine has several names, make sure that users connect to the service through the DNS host name that matches the common name in the certificate.
CVE numbers	
Affected IP addresses