Now from Symantec

VeriSign Authentication Services

脆弱性アセスメントレポート

www.foo.co.jp

IPアドレス：1.1.1.1

スキャン日：23-Oct-2012

シマンテック脆弱性アセスメントレポート

脆弱性アセスメントレポート

目次

概要

このレポートはSSLサーバ証明書の付加機能として提供される脆弱性アセスメントが検知した結果です。スキャン対象のウェブサイトの機密情報を含んでいますので、情報の取り扱いにはご注意ください。

免責条項

シマンテックのサービスを受けるにあたって、貴方は以下の内容および項目を理解し同意したものとします。
I)ウェブサイトにある全ての脆弱性を検知するものではありません。
II)検知した脆弱性やセキュリティの脅威を守ったり、改善したり、予防するものではありません。
III)シマンテックは提案された対応策で対応が完了することを保証または示すものではありません。
また、いかなる直接的、間接的、付帯的、特別な、懲罰的、結果的な損害を含み、お客様やその他の個人、団体に上記のI)、II)、III)にともなった、もしくは関連した損害または損失に対してシマンテックの役員、管理職、従業員とその関連会社は責任と義務を明確に否認します。

脆弱性アセスメントレポート概要

スキャンの結果、脆弱性が発見されました。脆弱性の詳細と対策については以下のページをご参照ください。

	2 重大な脆弱性	9 注意を要する脆弱性
ウェブ	0	0
ウェブアプリケーション	2	2
データベース	0	2
メール	0	0
ネットワーク	0	0
リモートアクセス	0	0
通信	0	5
ローカル	0	0
その他	0	0
総計	**2**	**9**

リスクレベル	内容(Definition)
重大な脆弱性 (Critical)	至急に対策を要する内容です。この脆弱性を利用して攻撃された場合、システムの改ざんや情報漏えいの被害につながる恐れがあります。すぐに開発会社や担当部門へ確認頂き、適切な対応をいただくことをお勧めします。
注意を要する脆弱性 (Informational)	直ちに対策を要す脆弱性ではありませんが、注意が必要な脆弱性を表示します。開発会社や担当部門へ確認をいただくことをお勧めします。

影響範囲	内容(Definition)
ウェブ	ウェブサーバ、ウェブサーバのプラグイン、アプリケーションサーバなど
ウェブアプリケーション	ウェブアプリケーション、ウェブ開発フレームワーク、CMSなど
データベース	データベースアプリケーション
メール	ウェブメール、SMTP、IMAP、POP3など
ネットワーク	DNS、LDAPなどのネットワークサービス、ルーターやファイアウォールの設定、SNMPなど
リモートアクセス サービス	VPN、Telnet、FTP、SSH、rlogin/RSH、rdesktop、x11のようなリモートアクセスサービス
通信	IRC、SSL、XMPPなどの通信やメッセージングサービス
ローカル	OSレベルや、外部からは利用できないシステム内部に存在する脆弱性
その他	上記の分類に入らないその他脆弱性

重大な脆弱性のアクションリスト

スキャンの結果、ウェブサイトに重大な脆弱性を検知しました。すぐに対策を行うべき脆弱性について、以下の通り影響範囲、原因、対策を表示します。

影響範囲	原因	対策方法	詳細
ウェブアプリケーション	Outdated Software	Upgrade to the latest version at http://www.php.net/downloads.php	VA-001
ウェブアプリケーション	Outdated Software	Upgrade to the latest version at http://www.php.net/downloads.php	VA-002

重大な脆弱性の詳細

スキャンの結果、ウェブサイトに重大な脆弱性を検知しました。重大な脆弱性の詳細は以下をご確認ください。

PHP Multiple Vulnerabilities	PORT(8080/TCP)
ID #	VA-001
影響範囲	ウェブアプリケーション
リスクのタイプ	Remote compromise
原因のタイプ	Outdated Software
脆弱性の詳細	The target system is identified running a PHP version prior to 5.2.11 that is prone to multiple vulnerabilities listed below: • Error in the 'php_openssl_apply_verification_policy' function that does not properly perform certificate validation. • Input validation error in the processing of 'exif' data. • Unspecified error exists related to the sanity check for the color index in the 'imagecolortransparent' function. Successful exploitation will allow the attackers to spoof certificates and can cause unknown impacts in the context of the web application. More detailed information at: • http://www.php.net/releases/5_2_11.php • http://www.php.net/ChangeLog-5.php#5.2.11 Details: PHP version 4.4.7 was detected on the host
必要になる行動	Upgrade to the latest version at http://www.php.net/downloads.php
参照	詳細は Appendix B - Technical References (VA-001) をご参照
検知日	23-Oct-2012

PHP Multiple Buffer Overflow Vulnerabilities	PORT(8080/TCP)
ID #	VA-002
影響範囲	ウェブアプリケーション
リスクのタイプ	Remote compromise
原因のタイプ	Outdated Software
脆弱性の詳細	PHP is prone to multiple buffer-overflow vulnerabilities. Successful exploits may allow attackers to execute arbitrary code in the context of applications using the vulnerable PHP functions. This may result in a compromise of the underlying system. Failed attempts may lead to a denial-ofservice condition. Versions prior to PHP 4.4.9 and PHP 5.2.8 are vulnerable. Details: PHP version 4.4.7 was detected on the host
必要になる行動	Upgrade to the latest version at http://www.php.net/downloads.php
参照	詳細は Appendix B - Technical References (VA-002) をご参照
検知日	23-Oct-2012

注意を要する脆弱性のアクションリスト

スキャンの結果、検知した「注意を要する脆弱性」のリストです。対象のウェブサイトへの影響範囲、原因、対策を表示します。

影響範囲	原因	対策方法	詳細
通信	Other	Always set the secure attribute when the cookie should be sent via HTTPS only.	VA-003
通信	Misconfiguration	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.	VA-004
通信	Misconfiguration	Purchase or generate a proper certificate for this service.	VA-005
データベース	Outdated Software	Upgrade MySQL to latest version at http://dev.mysql.com/downloads.	VA-006
データベース	Outdated Software	Upgrade MySQL to latest version at http://dev.mysql.com/downloads	VA-007
通信	Misconfiguration	Please make sure your HTTPS server is installed with all intermediary SSL certificates as well as the root SSL certificate.	VA-008
通信	Misconfiguration	Disable SSLv2	VA-009
ウェブアプリケーション	Outdated Software	Upgrade to the latest version at http://www.php.net/downloads.php	VA-010
ウェブアプリケーション	Outdated Software	Upgrade to PHP version 5.4.0 or later versions at http://www.php.net/downloads.php	VA-011

注意を要する脆弱性の詳細

スキャンの結果、検知した「注意を要する脆弱性」の詳細を示しました。ウェブサイトで利用している言語などの条件によっては悪用される危険性があるものやウェブサイト固有の環境・条件では脆弱性ではないものも含まれることがありますが、開発会社に相談するなど影響がないことを確認ください。

Missing Secure Attribute in an Encrypted Session (SSL) Cookie	**PORT(8443/TCP)**
ID #	VA-003
影響範囲	通信
リスクのタイプ	Other
原因のタイプ	Other
脆弱性の詳細	The flaw is caused due to SSL cookie is not using 'secure' attribute, which allows cookie to be passed to the server by the client over non-secure channels (http) and allows attacker to conduct session hijacking attacks. Details: Set-Cookie: PLESKSESSID=c5f552b650923ad321aa29062f176865; path=/
必要になる行動	Always set the secure attribute when the cookie should be sent via HTTPS only.
参照	詳細は Appendix B - Technical References (VA-003) をご参照
検知日	23-Oct-2012

SSL Certificate - Subject Common Name Does Not Match Server FQDN	**PORT(8443/TCP)**
ID #	VA-004
影響範囲	通信
リスクのタイプ	Other
原因のタイプ	Misconfiguration
脆弱性の詳細	The SSL certificates could not determine which is the primary certificate for the Web server. Make sure that the domain name entered above matches the common name of the certificate installed on the Web server. Details: Hostname: erne.es Common Name: plesk
必要になる行動	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.
参照	無し
検知日	29-Oct-2012

注意を要する脆弱性の詳細

SSL Certificate - Self-Signed Certificate Detection	PORT(8443/TCP)
ID #	VA-005
影響範囲	通信
リスクのタイプ	Other
原因のタイプ	Misconfiguration
脆弱性の詳細	When using a self-signed certificate, there is no chain of trust. The certificate has signed itself. The web browser will then issue a warning, telling you that the web site certificate cannot be verified. Therefore, you should not use self-signed certificates for professional use, as your visitors will not trust your web site to be safe. Overview: The ssl certificate on this Port is self signed. See also: http://en.wikipedia.org/wiki/Self-signed_certificate
必要になる行動	Purchase or generate a proper certificate for this service.
参照	無し
検知日	29-Oct-2012

MySQL MyISAM Table Privileges Secuity Bypass Vulnerability	PORT(3306/TCP)
ID #	VA-006
影響範囲	データベース
リスクのタイプ	Remote compromise
原因のタイプ	Outdated Software
脆弱性の詳細	The target system is identified running MySQL 4 (prior to 4.1.24) and (prior to 5.0.60) that is prone to a security-bypass vulnerability. An attacker can exploit this issue to gain access to table files created by other users, bypassing certain security restrictions. This issue was also assigned CVE-2008-4097 because CVE-2008-2079 was incompletely fixed, allowing symlink attacks. CVE-2008-4098 was assigned because fixes for the vector described in CVE-2008-4097 can also be bypassed. Details: MySQL version 5.0.45-community-nt was detected on the host
必要になる行動	Upgrade MySQL to latest version at http://dev.mysql.com/downloads.
参照	詳細は Appendix B - Technical References (VA-006) をご参照
検知日	23-Oct-2012

注意を要する脆弱性の詳細

MySQL Multiple Vulnerabilities	PORT(3306/TCP)
ID #	VA-007
影響範囲	データベース
リスクのタイプ	Remote compromise
原因のタイプ	Outdated Software
脆弱性の詳細	The target system is identified running MySQL 5.0.x before 5.0.91 and 5.1.x before 5.1.47 on all running platform, that is prone to multiple vulnerabilities. Successful exploitation could allow users to cause a denial of service and to execute arbitrary code. Details: MySQL version 5.0.45-community-nt was detected on the host
必要になる行動	Upgrade MySQL to latest version at http://dev.mysql.com/downloads
参照	詳細は Appendix B - Technical References (VA-007) をご参照
検知日	23-Oct-2012

Invalid SSL certificate chain	PORT(443/TCP)
ID #	VA-008
影響範囲	通信
リスクのタイプ	Other
原因のタイプ	Misconfiguration
脆弱性の詳細	Check whether an HTTPS client is able to establish a valid SSL certificate chain using the intermediary SSL certificates provided by an HTTP server. If your HTTPS server does not have all intermediate certificates installed, then the client would not be able to properly verify the server's Web Server Certificate and establish a trusted chain. This means that when visitors attempt to access your supposedly secure site, they will see a "Security Alert" indicating that "The security certificate was issued by a company you have not chosen to trust." Upon seeing this, the most likely action by potential customers is to take their businesses elsewhere.
必要になる行動	Please make sure your HTTPS server is installed with all intermediary SSL certificates as well as the root SSL certificate.
参照	無し
検知日	29-Oct-2012

注意を要する脆弱性の詳細

SSL v2 support detected	PORT(443/TCP)
ID #	VA-009
影響範囲	通信
リスクのタイプ	Other
原因のタイプ	Misconfiguration
脆弱性の詳細	The remote service accepts connections encrypted using SSL 2.0, which reportedly suffers from several cryptographic flaws and has been deprecated for several years. An attacker may be able to exploit these issues to conduct man-in-the-middle attacks or decrypt communications between the affected service and clients. Details: Accepted SSLv2 168 bits DES-CBC3-MD5 Accepted SSLv2 128 bits RC4-MD5
必要になる行動	Disable SSLv2
参照	無し
検知日	23-Oct-2012

PHP Security Bypass Vulnerability	PORT(8080/TCP)
ID #	VA-010
影響範囲	ウェブアプリケーション
リスクのタイプ	Remote compromise
原因のタイプ	Outdated Software
脆弱性の詳細	PHP is prone to a security-bypass vulnerability. Remote attackers can exploit this issue to bypass certain security restrictions and create arbitrary files in the context of the application. Versions prior to PHP 5.3.9 are vulnerable. Details: PHP version 4.4.7 was detected on the host
必要になる行動	Upgrade to the latest version at http://www.php.net/downloads.php
参照	詳細は Appendix B - Technical References (VA-010) をご参照
検知日	23-Oct-2012

注意を要する脆弱性の詳細

PHP Web Form Hash Collision Denial of Service Vulnerability	PORT(8080/TCP)
ID #	VA-011
影響範囲	ウェブアプリケーション
リスクのタイプ	Denial of service
原因のタイプ	Outdated Software
脆弱性の詳細	PHP before 5.3.9 computes hash values for form parameters without restricting the ability to trigger hash collisions predictably, which allows remote attackers to cause a denial of service (CPU consumption) by sending many crafted parameters. Details: PHP version 4.4.7 was detected on the host
必要になる行動	Upgrade to PHP version 5.4.0 or later versions at http://www.php.net/downloads.php
参照	詳細は Appendix B - Technical References (VA-011) をご参照
検知日	23-Oct-2012

Appendix A - システム環境情報

脆弱性アセスメントの対象システムのシステム環境に関する情報は以下の通りです。

ホストの詳細

パラメータ	値
ホスト名	www.foo.co.jp
IPアドレス	1.1.1.1

開いているポート

ポート	プロトコル	サービス	コメント
21	tcp	FTP	
25	tcp	SMTP	
53	udp	DOMAIN	
53	tcp	DOMAIN	
80	tcp	HTTP	
110	tcp	POP3	
139	tcp	NETBIOS-SSN	
143	tcp	IMAP	
443	tcp	HTTPS	
445	tcp	MICROSOFT-DS	
1433	tcp	MS-SQL-S	
3306	tcp	MYSQL	
3389	tcp	MS-WBT-SERVER	
8080	tcp	HTTP-ALT	
8443	tcp	PCSYNC-HTTPS	

Appendix B - 技術参照情報

脆弱性に関する詳細な説明、条件等は参照情報として、以下に説明リンクを用意(英語サイト) しています。日本語の解説や対策方法はCWE、CVE、BIDのコードを利用してJVN(Japan Vulnerability Notes) <https://jvn.jp/>や検索エンジンで調べてください。

重大な脆弱性

ID #	参照情報
VA-001	CVE-2009-3291 CVE-2009-3292 CVE-2009-3293 BID:36449
VA-002	CVE-2008-3659 CVE-2008-3658 BID:30649

注意を要する脆弱性

ID #	参照情報
VA-003	CVE-2004-0462 CWE-614
VA-006	CVE-2008-2079 CVE-2008-4097 CVE-2008-4098 BID:29106
VA-007	CVE-2010-1848 CVE-2010-1849 CVE-2010-1850
VA-010	CVE-2012-0057 BID:51806
VA-011	CVE-2011-4885

定義:

CVE CVE(Common Vulnerabilities and Exposures)は、個別製品中の脆弱性に一意の識別番号「CVE識別番号(CVE-ID)」を付与することにより、脆弱性対策情報同士の相互参照や関連付けに利用されています。

BID BID(Bugtraq ID)は、コンピューターの脆弱性を議論し公開する為の公開メーリングリストです。

CWE CWE(Common Weakness Enumeration)は、ソフトウェアにおけるセキュリティ上の弱点(脆弱性)の種類を識別するための共通の基準です。