GSX_MuroranIT_100IP

脆弱性の評価
SecureScout

レポート生成日:
Monday, March 25, 2013 10:44:12

Powered by

SecureScout

目次

レポートの要約

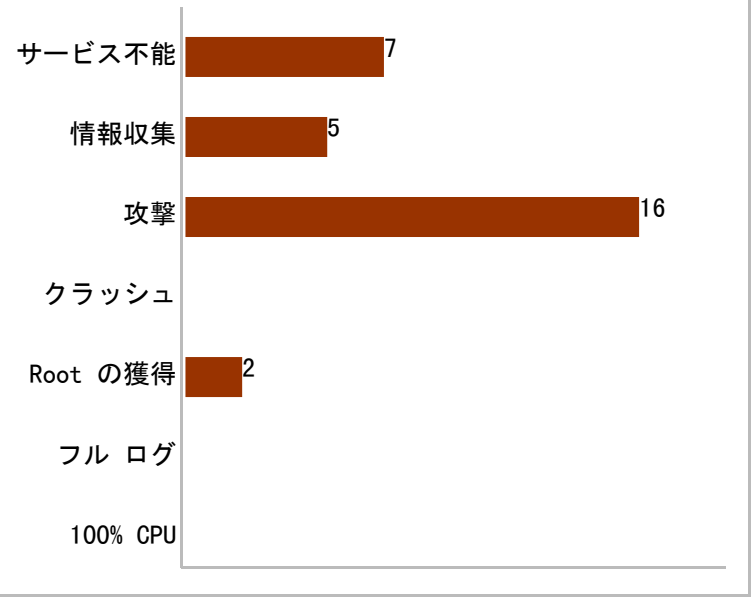
ユーザ名:	IWI_TY_121221
会社名:	GSX_MuroranIT_100IP
セッション ID:	101
セッション名:	mit
ジョブ ID:	472
ジョブ開始日時:	Monday, March 25, 2013 10:39:56
ジョブ終了日時:	Monday, March 25, 2013 10:43:59
SecureScout NX バージョン:	2.6.549.0
ポリシー:	安全なスキャン

一般情報

脆弱性			検出総数 : 22
	高リスク脆弱性	4	
	中リスク脆弱性	12	
	低リスク脆弱性	6	

セキュリティリスクの分類

ひとつの脆弱性はまた、ひとつ以上のセキュリティ上の潜在的危険性に関与しています。これらのリスクとその影響には情報収集、フルログ閲覧だけでなくサービス不能、ターゲットシステムのクラッシュ、rootの獲得ならびにその他手法による干渉が含まれます。結果は以下にある影響の区分に従い分類されます。以下の図における結果は、脆弱性による実際の影響を（SecureScout テストケースにおけるインパクトの区分に替えて）表すものです

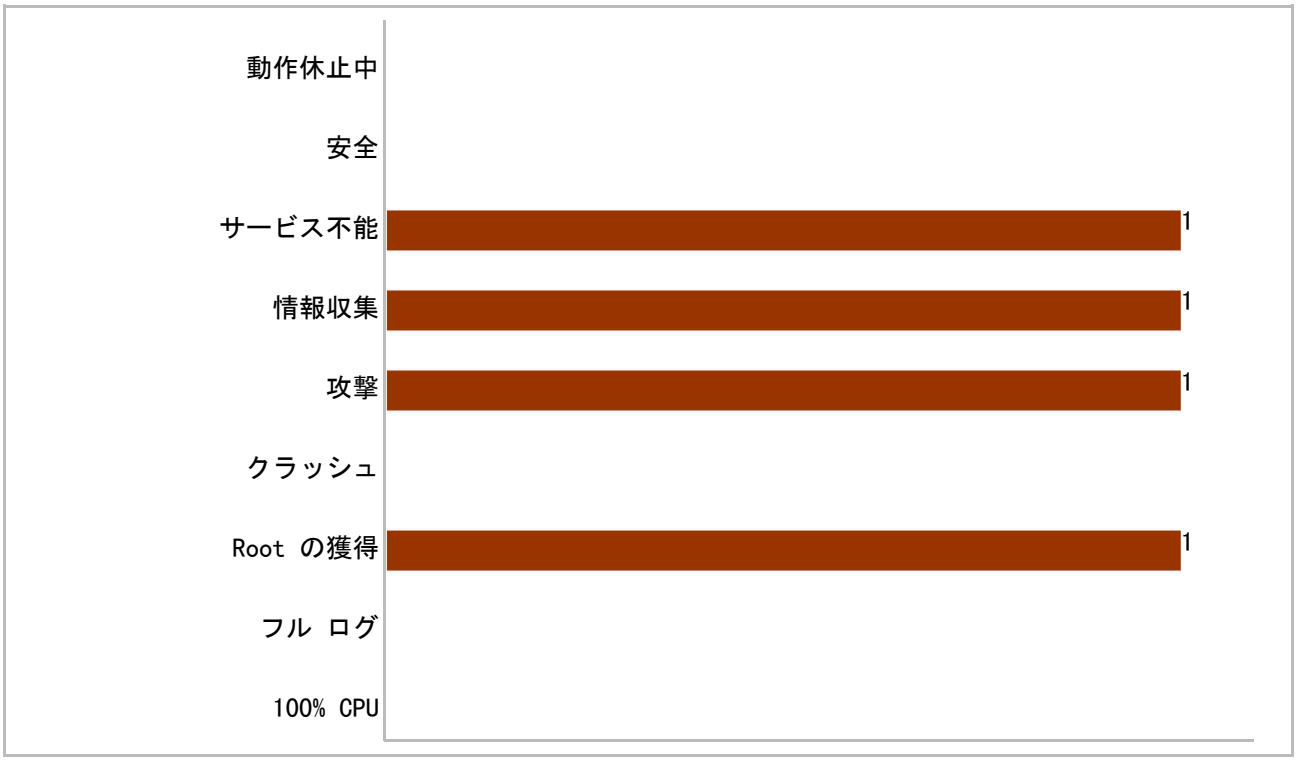


リスクの存在するホスト

テストされた 1 ホストにおいて、 SecureScout は 1 の脆弱なホスト ならびに 0 の動作していないホストを検出しました。 以下のグラフでは存在する脆弱性リスクの高い順にホストがカウントされています。

高リスクの存在するホスト	
1	
中リスクの存在するホスト	
0	
低リスクの存在するホスト	
0	
安全なホスト	
0	
動作していないホスト	
0	

以下のグラフでは脆弱性が (SecureScout テストケースにおけるインパクトの区分に替えて) 実際に与える影響に基づいた各セキュリティ項目における脆弱なホストがカウントされています。



テストされたホスト

IP アドレスによる分類に従い、ホストはそれぞれの名称（存在する場合）、リスク レベル、ならびに検出された脆弱性の総数とテストで用いられたテスト媒体（コンソール もしくは エージェント）を示します。

ホストの IP	名前	最大リスク	脆弱性数	アクセス実行
157.19.104.107	gateway107.csse.muroran-it.ac.jp		22	コンソール

ネットワーク情報

SecureScout テストは次の IP アドレスについて設定され実行されました:

テストされたポート :

TCP	1-1023
UDP	7, 9, 11, 13, 17, 19, 37, 42, 53, 67-69, 79, 88, 111, 113, 123, 135, 137-138, 161-162, 389-390, 396, 445, 464, 500, 512-514, 517-520, 525, 530-533, 540-541, 543-544, 546-547, 550, 554, 556, 560-561, 635, 640, 650, 666, 749, 750-751, 762, 1434, 2049

トレースルート

ターゲットに対するトレースルートはシステムならびにソフトウェアに関する潜在的な機密性の高い情報の提供を可能にします。 確信的なクラッカーはトレースルートすることで Web サーバを内部システムへの侵入突入口として使用するための十分な推論が可能です。 ルータ内に記録されている内部接続システムについてのデータ等の漏洩はクラッカーによるあなたのリソースのマッピング防止のため避けねばなりません。 システムがターゲット システムへ送信されたパケットの経路を辿ることが可能な場合、経路情報は以下に一覧表示されます:

ホストの IP	トレースルート
157.19.104.107	ﾎｽﾄ gateway107.csse.muroran-it.ac.jp への Traceroute : > 157.19.201.126 157.19.201.126 > gateway107.csse.muroran-it.ac.jp 157.19.104.107

オペレーティングシステムならびに Ping

脆弱性はオペレーティングシステムにより分類可能です。 オペレーティングシステム情報を識別することは侵入を試みる者にとって攻撃の焦点を高め、正確性を増す意味において有用です。 SecureScout はターゲットシステム上で実行しているオペレーティングシステムの検出を試行します。 ターゲットシステムより引き出された情報に基づく自動オペレーティングシステム検出機能は常に実施可能というわけではありません。 これはターゲットシステム上での一般的な安全レベルを高めるために有利に働くと捉えることができます。
Ping はシステムの存在を検査するために使用可能です; 大多数のシステムにおいて ping への応答は必要ではありません。 SecureScout は ping および/もしくは TCP ping リクエストによりターゲットシステムへの到達を試行します。 システムより応答がある場合、以下のテーブルに一覧表示されます。

検出された OS

オペレーティングシステム	%	
others	100 %	

注意: オペレーティングシステム総数の 5% 以下が "その他" のカテゴリーに含まれると示されています

Ping

Ping はシステムの存在を検査するために使用可能です; 大多数のシステムにおいて ping への応答は必要ではありません。 SecureScout は ping および/もしくは TCP ping リクエストによりターゲットシステムへの到達を試行します。 システムより応答がある場合、以下のテーブルに一覧表示されます

IP	オペレーティングシステム	Ping
157.19.104.107	NetBSD 5.0 - 5.99.5	可能

開いているポートとサービス

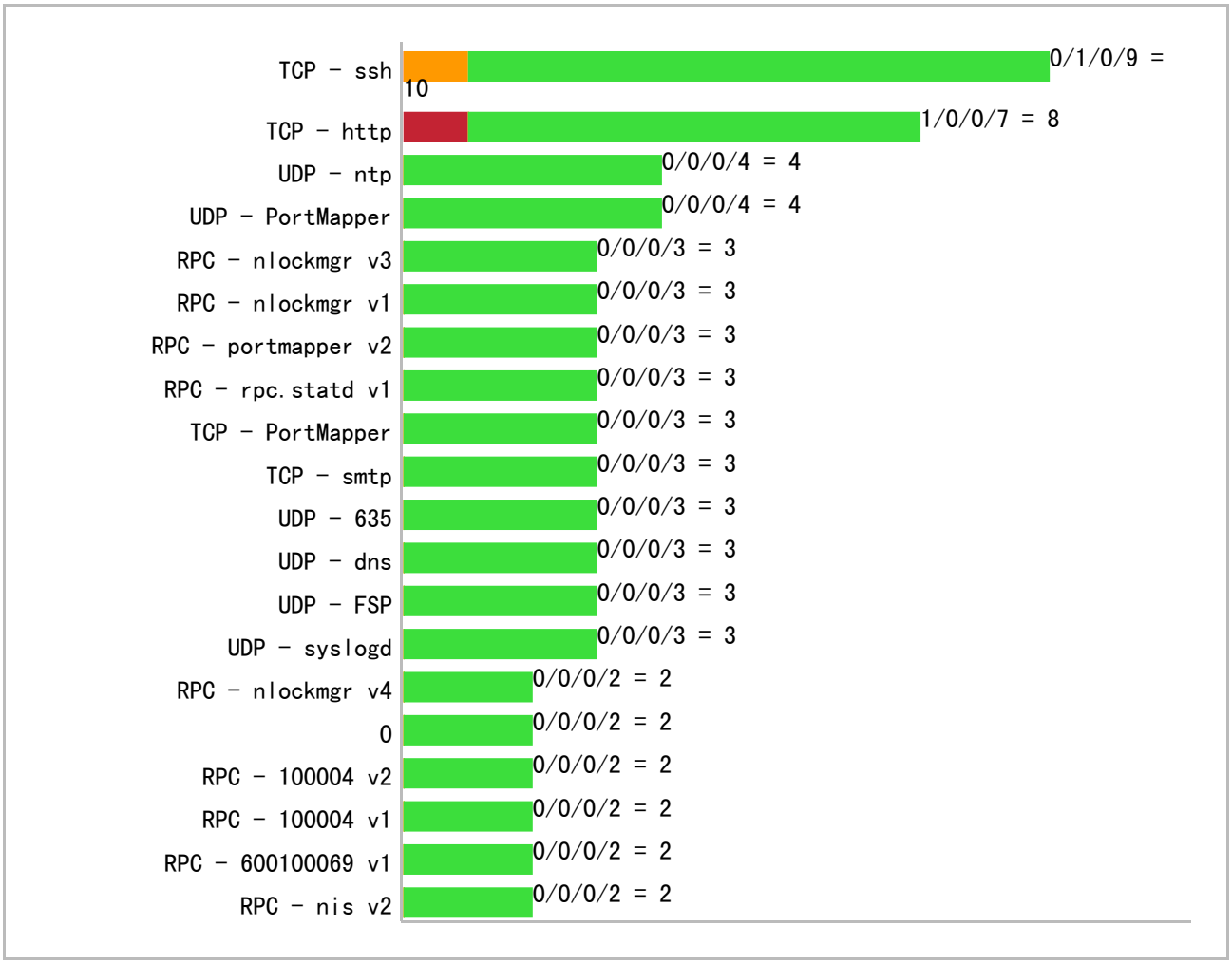
ポートはターゲット システム上のサービスへのインターフェースです。 最適なセキュリティ設定により、開いているポート数は最小限に抑えられつつ、システム管理は有効になり、コンピュータ システムに必要なサービスがサポートされます。

特定のテスト ケースは開かれた追加ポートを検出する可能性があります。

サービスのトップ 20 一覧

以下は、検出数が上位 20 位までのサービスを、検出総数の多いインスタンスの順（同数であれば高いリスクが多いインスタンスの順）に表示したものです。サービスの各インスタンスは、検出されたリスクのうち最も高いものとして表示されます。ターゲット上で開いている各ポートに対して（サービスに依存しない）テストケースによりチェックされた脆弱性に関するものは、表示されません。

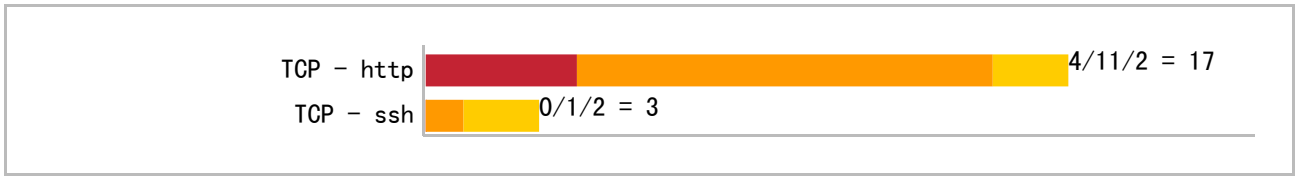
高（赤）/中（橙）/低（黄）/安全（緑）= 総数。



脆弱性ならびにサービス

以下は、検出された脆弱性数順（同数であれば高、中、低レベル数の順）にサービスを表示したものです。

高/中/低 = 総数。



開いてるポート一覧

テストされた IP レンジについて検出された開いているポートの一覧です。 記されているサービスは SecureScout により識別されたサービスです。

157.19.104.107		
(TCP/UDP/RPC)	ポート/RPC プログラム	確認されたサービス
TCP	22	ssh
TCP	80	http
TCP	873	rsyncd
UDP	67	bootps
UDP	68	bootpc

脆弱性

テストにて検出を受けた脆弱性がこのセクションに示されます。 脆弱性は次の高、中、低リスクの３項目に分類可能です。

高リスク脆弱性区分

SecureScout はホストを一方的および直接（他の脆弱性との組み合わせではなく）危険性に曝す全ての脆弱性を高リスクな脆弱性として表示します。危険に曝す例としては、データの窃盗、改竄あるいは削除、ホストの制御（他マシンへの無制限のハッキングあるいはバックドアの設置等)、または任意のコードを実行する脆弱性が挙げられます。

中リスク脆弱性区分

SecureScout は、脆弱性それ自身によってではなく（どのようにホストが危険に曝されるかの例は上記の高リスク脆弱性を参照してください）ホストを危険に曝す全ての脆弱性を中リスクの脆弱性として表示します。 しかしながら、中程度の脆弱性はホストを危険に曝すために少なくとも他の中程度の脆弱性と組み合わされる可能性があります。さらに、いくつかの低リスクの脆弱性から収集された情報と中リスクの脆弱性の組み合わせによりホストを危険に曝すことができます。SecureScout は、サービス不能攻撃を中リスクの脆弱性とみなします。

低リスク脆弱性区分

低リスクの脆弱性は、ホストがより危険に曝される影響を受けやすくします。(どのように ホストが危険に曝されるかの例は上記の高リスク脆弱性を参照してください。) 典型的な低リスクの脆弱性は、ホストあるいはそのオペレーティング環境についての過度の情報を提供していることです。 報告された全ての脆弱性をチェックし、少なくとも全ての高および中リスク脆弱性を修正してください。

高リスク脆弱性の一覧

名前	脆弱なホスト
Apache HTTP Server 'mod_proxy_ajp モジュール' におけるサービス不能の脆弱性 (CVE-2012-4557)	157.19.104.107
PHP 'sapi/cgi/cgi_main.c' における情報漏えいの脆弱性 (CVE-2012-1823)	157.19.104.107
phpMyAdmin PMA_Bookmark_get 関数において bookmark を生成する SQL クエリが実行される	157.19.104.107
phpMyAdmin において存在しないファイルへの直接リクエストを介し、インストールパスが挿入される	157.19.104.107

中リスク脆弱性の一覧

名前	脆弱なホスト
Apache APR 'apr_fnmatch()' におけるサービス不能の脆弱性	157.19.104.107
Apache HTTP Server における 'mod_proxy' リバースプロキシの情報漏えいの脆弱性	157.19.104.107
Apache HTTP Server の 'httpOnly' Cookie による情報漏えいの脆弱性 (CVE-2012-0053)	157.19.104.107

中リスク脆弱性の一覧

名前	脆弱なホスト
Apache HTTP Server の 'LD LIBRARY PATH' における不安定なライブラリのロードによる脆弱性 (CVE-2012-0883)	157.19.104.107
Apache HTTP Server の Scoreboard によるローカルセキュリティ迂回の脆弱性 (CVE-2012-0031)	157.19.104.107
Apache HTTP Server 不正な形式の URI 'mod proxy' による脆弱性	157.19.104.107
Apache HTTP サーバにおけるサービス不能の複数の脆弱性	157.19.104.107
HTTP TRACE メソッドにおけるクロスサイト トレーシングの脆弱性	157.19.104.107
OpenSSH "X11UseLocalhost" による X11 転送のセキュリティ問題	157.19.104.107
PHP 'phar/tar.c' におけるヒープ バッファ オーバーフローの脆弱性 (CVE-2012-2386)	157.19.104.107
PHP 'rfc1867.c ' におけるディレクトリ トラバーサルの脆弱性 (CVE-2012-1172)	157.19.104.107
PHP における深い再帰への保護を行わない脆弱性	157.19.104.107

低リスク脆弱性の一覧

名前	脆弱なホスト
Apache HTTP Server の mod log config におけるサービス不能の脆弱性 (CVE-2012-0021)	157.19.104.107
HTTP バナーの露出	157.19.104.107
ICMP タイムスタンプ返信の脆弱性	157.19.104.107
OpenSSH Forced command 処理における情報漏洩の脆弱性 (CVE-2012-0814)	157.19.104.107
SSH サービスが稼動しています	157.19.104.107
Traceroute が利用可能	157.19.104.107

高リスク脆弱性

	Apache HTTP Server 'mod_proxy_ajp モジュール' におけるサービス不能の脆弱性 (CVE-2012-4557)	CVE id	CVE-2012-4557
		SecureScout id	13988
説明	Apache HTTP Server 2.2.12 から 2.2.21 の mod_proxy_ajp モジュールは、長いリクエスト処理時間を検出した場合、ワーカー ノードをエラー状態に配置します。それにより、リモートの攻撃者が高いリクエストを用いて、サービス不能 (ワーカー 消費) を引き起こす可能性があります。		
参照	* CONFIRM: http://httpd.apache.org/security/vulnerabilities_22.html#2.2.22 * CONFIRM: http://svn.apache.org/viewvc?view=revision &revision=1227298 * CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=871685 * DEBIAN: DSA-2579 http://www.debian.org/security/2012/dsa-2579		
対策	Apache をバージョン 2.2.22 もしくはこれ以降に更新してください。 詳細については参照を確認ください。		
以下で検出: 157.19.104.107 - ポート: 80			
HTTP バナーは: Apache/2.2.17 (Unix) DAV/2 PHP/5.3.22			

	PHP 'sapi/cgi/cgi_main.c' における情報漏えいの脆弱性 (CVE-2012-1823)	CVE id	CVE-2012-1823
		SecureScout id	19897
説明	PHP 5.3.12 未満および 5.4.2 未満の 5.4.x の sapi/cgi/cgi_main.c は CGIスクリプト(別名 php-cgi) として設定された際に、= (等号) 文字列を欠いたクエリ文字列を適切に処理しません。それにより、リモートの攻撃者が 'd' ケース用の特定の php_getopt の省略が不足していることに関連したクエリ文字列内にコマンド ライン オプションを置くことで、任意のコードを実行する可能性があります。		
参照	* MISC: http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/ * CONFIRM: http://www.php.net/ChangeLog-5.php#5.4.2 * CONFIRM: http://www.php.net/archive/2012.php#id2012-05-03-1 * CONFIRM: https://bugs.php.net/bug.php?id=61910 * CONFIRM: https://bugs.php.net/patch-display.php?bug_id=61910 &patch=cgi.diff &revision=1335984315 &display=1 * HP: HPSBMU02786 http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03360041 * REDHAT: RHSA-2012:0546 http://www.redhat.com/support/errata/RHSA-2012-0546.html * REDHAT: RHSA-2012:0547 http://www.redhat.com/support/errata/RHSA-2012-0547.html * REDHAT: RHSA-2012:0568 http://www.redhat.com/support/errata/RHSA-2012-0568.html * CERT-VN: VU#520827		

	PHP 'sapi/cgi/cgi_main.c' における情報漏えいの脆弱性 (CVE-2012-1823)	CVE id	CVE-2012-1823
		SecureScout id	19897
	http://www.kb.cert.org/vuls/id/520827 * SECUNIA: 49014 http://secunia.com/advisories/49014 * SECUNIA: 49065 http://secunia.com/advisories/49065 * SECUNIA: 49087 http://secunia.com/advisories/49087		
対策	バージョン 5.4.3 もしくはこれ以降に更新してください。 詳細については参照を確認ください。		
以下で検出: 157.19.104.107 - ポート: 80			
HTTP バナーは: Apache/2.2.17 (Unix) DAV/2 PHP/5.3.22 PHP 検出バージョン: 5.3.22			

	phpMyAdmin PMA_Bookmark_get 関数において bookmark を生成する SQL クエリが実行される	CVE id	CVE-2011-0987
		SecureScout id	19629
説明	phpMyAdmin 2.11.11.3 未満の 2.11.x および 3.3.9.2 未満の 3.3.x の libraries/bookmark.lib.php 内の PMA_Bookmark_get 関数では、bookmark クエリを適切に制限しません。リモート認証されたユーザが bookmark を生成することで、別のユーザにて SQL クエリを実行することがより簡単になります。		
参照	* CONFIRM: http://phpmyadmin.git.sourceforge.net/git/gitweb.cgi?p=phpmyadmin/phpmyadmin;a=commit;h=a5464b4daff0059cdf8c9e5f4d54a80e2dd2a5b0 * CONFIRM: http://www.phpmyadmin.net/home_page/security/PMASA-2011-2.php * DEBIAN: DSA-2167 http://www.debian.org/security/2011/dsa-2167 * FEDORA: FEDORA-2011-1373 http://lists.fedoraproject.org/pipermail/package-announce/2011-February/054349.html * FEDORA: FEDORA-2011-1408 http://lists.fedoraproject.org/pipermail/package-announce/2011-February/054355.html * FEDORA: FEDORA-2011-1282 http://lists.fedoraproject.org/pipermail/package-announce/2011-March/054525.html * MANDRIVA: MDVSA-2011:026 http://www.mandriva.com/security/advisories?name=MDVSA-2011:026 * BID: 46359 http://www.securityfocus.com/bid/46359 * SECUNIA: 43324 http://secunia.com/advisories/43324 * SECUNIA: 43391 http://secunia.com/advisories/43391 * SECUNIA: 43478 http://secunia.com/advisories/43478 * VUPEN: ADV-2011-0381 http://www.vupen.com/english/advisories/2011/0381 * VUPEN: ADV-2011-0385		

	phpMyAdmin PMA_Bookmark_get 関数において bookmark を生成する SQL クエリが実行される	CVE id	CVE-2011-0987
		SecureScout id	19629
	http://www.vupen.com/english/advisories/2011/0385 * VUPEN: ADV-2011-0409 http://www.vupen.com/english/advisories/2011/0409 * VUPEN: ADV-2011-0512 http://www.vupen.com/english/advisories/2011/0512 * VUPEN: ADV-2011-0570 http://www.vupen.com/english/advisories/2011/0570 * XF: phpmyadmin-bookmark-security-bypass(65390) http://xforce.iss.net/xforce/xfdb/65390		
対策	phpmyadmin を 2.11.11.2 以降の 2.11.x および 3.3.9.1 以降の 3.3.x にアップグレードしてください。 詳細については参照を確認ください。		
以下で検出: 157.19.104.107 - ポート: 80			
phpmyadmin vulnerable version found			

	phpMyAdmin において存在しないファイルへの直接リクエストをパスが挿入される	CVE id	CVE-2011-0986
		SecureScout id	19628
説明	phpMyAdmin 2.11.11.2 未満の 2.11.x および 3.3.9.1 未満の 3.3.x では、(1) README、(2) ChangeLog および (3) LICENSE ファイルが欠落していることを適切に処理しません。 README、ChangeLog あるいは LICENSE ファイルが、(ディストリビュータによって) それらの本来の場所から取り除かれた場合、これらのファイルを表示するために使用されるスクリプトにより、それらのフルパスが表示され、さらなる可能性のある攻撃につながります。		
参照	* CONFIRM: http://phpmyadmin.git.sourceforge.net/git/gitweb.cgi?p=phpmyadmin/phpmyadmin;a=commit;h=035d002db1e1201e73e560d7d98591563b506a83 * CONFIRM: http://www.phpmyadmin.net/home_page/security/PMASA-2011-1.php * FEDORA: FEDORA-2011-1373 http://lists.fedoraproject.org/pipermail/package-announce/2011-February/054349.html * FEDORA: FEDORA-2011-1408 http://lists.fedoraproject.org/pipermail/package-announce/2011-February/054355.html * MANDRIVA: MDVSA-2011:026 http://www.mandriva.com/security/advisories?name=MDVSA-2011:026 * SECUNIA: 43478 http://secunia.com/advisories/43478 * VUPEN: ADV-2011-0385 http://www.vupen.com/english/advisories/2011/0385 * XF: phpmyadmin-readme-path-disclosure(65424) http://xforce.iss.net/xforce/xfdb/65424		
対策	phpmyadmin を 2.11.11.2 以降の 2.11.x および 3.3.9.1 以降の 3.3.x にアップグレードしてください。 詳細については参照を確認ください。		

	phpMyAdmin において存在しないファイルへの直接リクエストをパスが挿入される	CVE id	CVE-2011-0986
		SecureScout id	19628
以下で検出: 157.19.104.107 - ポート: 80			
phpmyadmin vulnerable version found			

中リスク脆弱性

	Apache APR 'apr_fnmatch()' におけるサービス不能の脆弱性	CVE id	CVE-2011-0419
		SecureScout id	19565
説明	Apache APR は、攻撃者がサービス不能状態を引き起こす脆弱性に陥る傾向があります。 Apache Portable Runtime (APR) 1.4.3 未満のライブラリと Apache HTTP Server 2.2.18 未満の apr_fnmatch.c 内の fnmatch および NetBSD 5.1、OpenBSD 4.8、FreeBSD、Apple Mac OS X 10.6、Oracle Solaris 10 および Android の libc 内の fnmatch.c におけるのスタック浪費の脆弱性により、コンテキストに依存した攻撃者が、第一引数内の *? シーケンスを用いて、サービス不能 (CPU およびメモリの浪費) を引き起こす可能性があります。本件は、httpd 内の mod_autoindex に対する攻撃によって実証済みです。		
参照	* SREASONRES: 20110512 Multiple Vendors libc/fnmatch(3) DoS (incl apache) http://securityreason.com/achievement_securityalert/98 * MLIST: [dev] 20110510 Re: Apache Portable Runtime 1.4.4 [...] Released http://www.mail-archive.com/dev@apr.apache.org/msg23961.html * MLIST: [dev] 20110510 Re: fnmatch rewrite in apr, apr 1.4.3 http://www.mail-archive.com/dev@apr.apache.org/msg23960.html * MLIST: [dev] 20110511 Re: Apache Portable Runtime 1.4.4 [...] Released http://www.mail-archive.com/dev@apr.apache.org/msg23976.html * MISC: http://cxib.net/stuff/apache.fnmatch.phps * CONFIRM: http://cvsweb.netbsd.org/bsdweb.cgi/src/lib/libc/gen/fnmatch.c#rev1.22 * CONFIRM: http://httpd.apache.org/security/vulnerabilities_22.html * CONFIRM: http://svn.apache.org/viewvc/apr/apr/branches/1.4.x/strings/apr_fnmatch.c?r1=731029 &r2=1098902 * CONFIRM: http://svn.apache.org/viewvc?view=revision &revision=1098188 * CONFIRM: http://svn.apache.org/viewvc?view=revision &revision=1098799 * CONFIRM: http://www.apache.org/dist/apr/Announcement1.x.html * CONFIRM: http://www.apache.org/dist/apr/CHANGES-APR-1.4 * CONFIRM: http://www.apache.org/dist/httpd/Announcement2.2.html * CONFIRM: http://www.openbsd.org/cgi-bin/cvsweb/src/lib/libc/gen/fnmatch.c#rev1.15 * CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=703390 * CONFIRM: http://support.apple.com/kb/HT5002?viewlocale=ja_JP * APPLE: APPLE-SA-2011-10-12-3 http://lists.apple.com/archives/Security-announce/2011//Oct/msg00003.html * DEBIAN: DSA-2237 http://www.debian.org/security/2011/dsa-2237		

	Apache APR 'apr_fnmatch()' におけるサービス不能の脆弱性	CVE id	CVE-2011-0419
		SecureScout id	19565
	* HP: HPSBUX02702 http://marc.info/?l=bugtraq &m=131551295528105 &w=2 * HP: HPSBUX02707 http://marc.info/?l=bugtraq &m=131731002122529 &w=2 * MANDRIVA: MDVSA-2011:084 http://www.mandriva.com/security/advisories?name=MDVSA-2011:084 * REDHAT: RHSA-2011:0507 http://www.redhat.com/support/errata/RHSA-2011-0507.html * REDHAT: RHSA-2011:0896 http://www.redhat.com/support/errata/RHSA-2011-0896.html * REDHAT: RHSA-2011:0897 http://www.redhat.com/support/errata/RHSA-2011-0897.html * SECTRACK: 1025527 http://securitytracker.com/id?1025527 * SECUNIA: 44490 http://secunia.com/advisories/44490 * SECUNIA: 44564 http://secunia.com/advisories/44564 * SECUNIA: 44574 http://secunia.com/advisories/44574 * SREASON: 8246 http://securityreason.com/securityalert/8246		
対策	Apache のバージョンを 2.2.19 もしくはこれ以降に更新してください。APR リリース 1.4.5 には httpd 2.2.19 がバンドルされています。 詳細については参照を確認ください。		
以下で検出: 157.19.104.107 - ポート: 80			
HTTP バナーは: Apache/2.2.17 (Unix) DAV/2 PHP/5.3.22			

	Apache HTTP Server における 'mod_proxy' リバース プロキシの情報漏えいの脆弱性	CVE id	CVE-2011-3368
		SecureScout id	19572
説明	Apache HTTP Server 1.3.x から 1.3.42、2.0.x から 2.0.64、2.2.x から 2.2.21 の mod_proxy モジュールは、リバース プロキシ設定用の (1) RewriteRule および (2) ProxyPassMatch パターンマッチの用法と適切に情報をやりとりしません。それにより、リモートの攻撃者が最初の @（アットマーク）文字を含んだ不正な形式の URI を用いて、インターネット サーバへリクエストを送信する可能性があります。		
参照	* EXPLOIT-DB: 17969 http://www.exploit-db.com/exploits/17969 * FULLDISC: 20111005 Apache HTTP Server: mod_proxy reverse proxy exposure (CVE-2011-3368) http://seclists.org/fulldisclosure/2011/Oct/232 * MLIST: [announce] 20111005 Advisory: mod_proxy reverse proxy exposure (CVE-2011-3368) http://web.archiveorange.com/archive/v/ZySOhzECD5zzb2NkvQlt * MISC: http://www.contextis.com/research/blog/reverseproxybypass/ * CONFIRM: http://svn.apache.org/viewvc?view=revision &revision=1179239 * CONFIRM:		

	Apache HTTP Server における 'mod_proxy' リバース プロキシの情報漏えいの脆弱性	CVE id	CVE-2011-3368
		SecureScout id	19572

	https://bugzilla.redhat.com/show_bug.cgi?id=740045 * AIXAPAR: SE49723 http://www-01.ibm.com/support/docview.wss?uid=nas2064c7e5f53452ff686257927003c8d42 * AIXAPAR: SE49724 http://www-01.ibm.com/support/docview.wss?uid=nas2b7c57b1f1035675186257927003c8d48 * MANDRIVA: MDVSA-2011:144 http://www.mandriva.com/security/advisories?name=MDVSA-2011:144 * REDHAT: RHSA-2011:1391 http://www.redhat.com/support/errata/RHSA-2011-1391.html * REDHAT: RHSA-2011:1392 http://www.redhat.com/support/errata/RHSA-2011-1392.html * BID: 49957 http://www.securityfocus.com/bid/49957 * SECTRACK: 1026144 http://www.securitytracker.com/id?1026144 * SECUNIA: 46288 http://secunia.com/advisories/46288 * SECUNIA: 46414 http://secunia.com/advisories/46414 * XF: apache-modproxy-information-disclosure(70336) http://xforce.iss.net/xforce/xfdb/70336
対策	Apache をバージョン 1.3.35、2.0.58、2.2.2 もしくはこれら以降に更新してください。 詳細については参照を確認ください。
以下で検出: 157.19.104.107 - ポート: 80	
HTTP バナーは: Apache/2.2.17 (Unix) DAV/2 PHP/5.3.22	

	Apache HTTP Server の 'httpOnly' Cookie による情報漏えいの脆弱性 (CVE-2012-0053)	CVE id	CVE-2012-0053
		SecureScout id	19869

説明	Apache HTTP Server 2.2.x から 2.2.21 の protocol.c では、Bad リクエスト (別名 400) エラーの生成中に、ヘッダ情報を適切に制限しません。それにより、リモートの攻撃者が細工された Web スクリプトと協力する (1) 長いもしくは (2) 不正な形式のヘッダーを含んだベクタを用いて、HTTPOnly cookie の値を獲得する可能性があります。
参照	* CONFIRM: http://httpd.apache.org/security/vulnerabilities_22.html * CONFIRM: http://svn.apache.org/viewvc?view=revision &revision=1235454 * CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=785069 * REDHAT: RHSA-2012:0128 http://www.redhat.com/support/errata/RHSA-2012-0128.html * SUSE: openSUSE-SU-2012:0314 http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.html * BID: 51706 http://www.securityfocus.com/bid/51706

	Apache HTTP Server の 'httpOnly' Cookie による情報漏えいの脆弱性 (CVE-2012-0053)	CVE id	CVE-2012-0053
		SecureScout id	19869
対策	Apache をバージョン 2.2.22 もしくはこれ以降に更新してください。 詳細については参照を確認ください。		
以下で検出: 157.19.104.107 - ポート: 80			
HTTP バナーは: Apache/2.2.17 (Unix) DAV/2 PHP/5.3.22			

	Apache HTTP Server の 'LD_LIBRARY_PATH' における不安定なライブラリのロードによる脆弱性 (CVE-2012-0883)	CVE id	CVE-2012-0883
		SecureScout id	19855
説明	Apache HTTP Server 2.4.2 未満の envvars (別名 envvars-std) は LD_LIBRARY_PATH に ゼロ サイズのディレクトリ名を置きます。それにより、ローカル ユーザが apachectl が実行されている際に、現在のワーキング ディレクトリ内のトロイの木馬 DSO を用いて、権限を獲得する可能性があります。		
参照	* MLIST: [dev] 20120417 [ANNOUNCEMENT] Apache HTTP Server 2.4.2 Released http://article.gmane.org/gmane.comp.apache.devel/48158 * CONFIRM: http://svn.apache.org/viewvc?view=revision &revision=1296428 * CONFIRM: http://www.apache.org/dist/httpd/Announcement2.4.html		
対策	Apache をバージョン 2.4.2 もしくはこれ以降に更新してください。 詳細については参照を確認ください。		
以下で検出: 157.19.104.107 - ポート: 80			
HTTP バナーは: Apache/2.2.17 (Unix) DAV/2 PHP/5.3.22			

	Apache HTTP Server の Scoreboard によるローカルセキュリティ迂回の脆弱性 (CVE-2012-0031)	CVE id	CVE-2012-0031
		SecureScout id	19820
説明	Apache HTTP Server 2.2.21 およびそれ以前の scoreboard.c により、ローカルのユーザが scoreboard の共有メモリセグメント内の特定の種類のフィールドを修正することにより、サービス不能を引き起こしたり、場合によってはその他の不特定のインパクトを与える可能性があります。		
参照	* MISC: http://www.halfdog.net/Security/2011/ApacheScoreboardInvalidFreeOnShutdown/ * CONFIRM: http://svn.apache.org/viewvc?view=revision &revision=1230065 * CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=773744 * REDHAT: RHSA-2012:0128 http://www.redhat.com/support/errata/RHSA-2012-0128.html * SUSE: openSUSE-SU-2012:0314 http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.html * BID: 51407 http://www.securityfocus.com/bid/51407 * SECUNIA: 47410 http://secunia.com/advisories/47410		
対策	Apache をバージョン 2.2.22 もしくはこれ以降に更新してください。 詳細については参照を確認ください。		
以下で検出: 157.19.104.107 - ポート: 80			
HTTP バナーは: Apache/2.2.17 (Unix) DAV/2 PHP/5.3.22			

	Apache HTTP Server 不正な形式の URI 'mod_proxy' による脆弱性	CVE id	CVE-2011-4317
		SecureScout id	19667
説明	Apache HTTP Server の 1.3.42 までの 1.3.x、2.0.64 までの 2.0.x および 2.2.21 までの 2.2.x の mod_proxy module は、リビジョン 1179239 のパッチが当てられた際に、リバース プロキシの設定用の (1) RewriteRule および (2) ProxyPassMatch パターンと適切に情報のやり取りを行いません。それにより、リモートの攻撃者が無効な位置に @ (アットマーク) 文字列および : (コロン) 文字列を含んだ不正な形式の URI を用いて、イントラネット サーバへリクエストを送信する可能性があります。		
参照	* MISC: https://community.qualys.com/blogs/securitylabs/2011/11/23/apache-reverse-proxy-bypass-issue * CONFIRM: http://thread.gmane.org/gmane.comp.apache.devel/46440 * CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=756483 * URL: cve-2011-4317 https://community.qualys.com/blogs/securitylabs/tags/cve-2011-4317		
対策	Apache のバージョンを 1.3.42 までの 1.3.x、2.0.64 までの 2.0.x および 2.2.21 までの 2.2.xもしくはこれ以降に更新してください。 詳細については参照を確認ください。		
以下で検出: 157.19.104.107 - ポート: 80			
HTTP バナーは: Apache/2.2.17 (Unix) DAV/2 PHP/5.3.22			

	Apache HTTP サーバにおけるサービス不能の複数の脆弱性	CVE id	CVE-2011-3192
		SecureScout id	19493
説明	Apache HTTP 1.3.x、2.0.64 までの 2.0.x および 2.2.19 までの 2.2.x 内の byterange フィルタにおいて、2011 年 8 月に一般的に悪用されているように、リモートの攻撃者が複数の重複する範囲を表現するレンジ ヘッダーを用いて、サービス不能 (メモリおよび CPU 浪費) を引き起こす可能性があります。これは CVE-2007-0086 とは異なる脆弱性です。		
参照	* EXPLOIT-DB: 17696 http://www.exploit-db.com/exploits/17696 * FULLDISC: 20110820 Apache Killer http://seclists.org/fulldisclosure/2011/Aug/175 * FULLDISC: 20110824 Re: Apache Killer http://archives.neohapsis.com/archives/fulldisclosure/2011-08/0285.html * MLIST: [announce] 20110824 Advisory: Range header DoS vulnerability Apache HTTPD 1.3/2.x ¥(CVE-2011-3192¥) http://mail-archives.apache.org/mod_mbox/httpd-announce/201108.mbox/%3c20110824161640.122D387DD@minotaur.apache.org%3e * CONFIRM: http://www.gossamer-threads.com/lists/apache/dev/401638 * CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=732928 * CONFIRM: https://issues.apache.org/bugzilla/show_bug.cgi?id=51714 * SECTRACK: 1025960 http://securitytracker.com/id?1025960		

	Apache HTTP サーバにおけるサービス不能の複数の脆弱性	CVE id	CVE-2011-3192
		SecureScout id	19493
	* SECUNIA: 45606 http://secunia.com/advisories/45606 * BID: 49303 http://www.securityfocus.com/bid/49303		
対策	Apache のバージョンを 2.2.20 もしくはこれ以降に更新してください。 詳細については参照を確認ください。		
以下で検出: 157.19.104.107 - ポート: 80			
HTTP バナーは: Apache/2.2.17 (Unix) DAV/2 PHP/5.3.22			

	HTTP TRACE メソッドにおけるクロスサイト トレーシングの脆弱性	CVE id	CVE-2004-2320 CVE-2005-3398 CVE-2005-3498
		SecureScout id	17623
説明	TRACE は、HTTP プロトコル バージョン 1.1 で利用可能な HTTP のメソッドです。このメソッドは通常 HTTP サーバにおいてデフォルトで利用可能です。このメソッドの目的は、クライアントからのリクエストに対し echo を実施することです。 このメソッドは、HTTP ヘッダ内のクライアントから送信された情報を引き出すために用いられる可能性があります。ブラウザが GET ならびに POST 以外のメソッドをサポートしないため、この脆弱性の悪用には ActiveX の利用のような特別な技術が必要となります。		
参照	* MISC: Cross-Site Tracing http://www.cgisecurity.com/whitehat-mirror/WhitePaper_screen.pdf * MISC: Mitigating Cross-site Scripting With HTTP-only Cookies http://msdn.microsoft.com/en-us/library/ms533046.aspx * BEA: BEA04-48.01 http://dev2dev.bea.com/pub/advisory/68 * CERT-VN: VU#867593 http://www.kb.cert.org/vuls/id/867593 * BID: 9506 http://www.securityfocus.com/bid/9506 * OSVDB: 3726 http://www.osvdb.org/3726 * SECTRACK: 1008866 http://www.securitytracker.com/alerts/2004/Jan/1008866.html * SECUNIA: 10726 http://secunia.com/advisories/10726 * XF: weblogic-trace-xss(14959) http://xforce.iss.net/xforce/xfdb/14959 * SUNALERT: 102016 http://sunsolve.sun.com/search/document.do?assetkey=1-26-102016-1 * BID: 15222 http://www.securityfocus.com/bid/15222 * FRSIRT: ADV-2005-2226 http://www.frsirt.com/english/advisories/2005/2226 * OVAL: oval:org.mitre.oval:def:1445 http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1445 * SECTRACK: 1015112		

	HTTP TRACE メソッドにおけるクロスサイトトレーシングの脆弱性	CVE id	CVE-2004-2320 CVE-2005-3398 CVE-2005-3498
		SecureScout id	17623

	http://securitytracker.com/id?1015112 * SECUNIA: 17334 http://secunia.com/advisories/17334 * CONFIRM: http://www-1.ibm.com/support/docview.wss?rs=180 &uid=swg27004980 * AIXAPAR: PK11017 http://www-1.ibm.com/support/docview.wss?uid=swg24010781 * BID: 15303 http://www.securityfocus.com/bid/15303 * FRSIRT: ADV-2005-2291 http://www.frsirt.com/english/advisories/2005/2291 * SECTRACK: 1015134 http://securitytracker.com/id?1015134
対策	TRACE 手法の使用を認めないでください。 Apache については、以下から入手可能なモジュール mod_rewrite を使用してください http://httpd.apache.org/docs/mod/mod_rewrite.html TRACE を認めないために、以下を実施してください: RewriteEngine On RewriteCond %{REQUEST_METHOD} ^TRACE RewriteRule .* - [F] Microsoft IIS の場合、例えば URL Scan を使用してください。このツールはこちらで入手可能です http://www.microsoft.com/technet/security/tools/urlscan.mspx URLScan の使用法および URL Scan が拒絶する HTTP ヘッダの定義方法についての情報は以下を参照してください http://support.microsoft.com/default.aspx?scid=kb;en-us;326444 * 詳細については参照を確認ください。
以下で検出: 157.19.104.107 - ポート: 80	
TRACE / HTTP/1.0 XST: SecureScout TC: 17623 ｺﾝﾃﾝﾂに関する HTTP ｻｰﾊﾞ応答: http/1.1 200 ok date: mon, 25 mar 2013 01:41:46 gmt server: apache/2.2.17 (unix) dav/2 php/5.3.22 connection: close content-type: message/http trace / http/1.0 xst: securescout tc: 17623	

	OpenSSH "X11UseLocalhost" による X11 転送のセキュリティ問題	CVE id	CVE-2008-3259
		SecureScout id	12157

説明	SO_REUSEADDR 設定で既にバインドされたポートに対してバインド(2)を試行する際、

	OpenSSH "X11UseLocalhost" による X11 転送のセキュリティ問題	CVE id	CVE-2008-3259
		SecureScout id	12157
	たいていのオペレーティング システムは、有効なユーザ id が以前のバインド (BSD から派生したシステムに共通) に対応しているか、あるいは バインド アドレスが重複していないか (Linux と Solaris) をチェックします。 HP/UX のようないくつかのオペレーティング システムは、これらのチェックを行わないため、sshd_config(5) オプション X11UseLocalhost が "no" に設定されている場合、X11 中間者攻撃に対し脆弱です。これにより、攻撃者がより具体的なバインドを確立して、sshd ワイルドカード リスナよりも優先されて使用される可能性があります。 現在の BSD オペレーティング システム、Linux、OS X および Solaris は、上記のチェックを実行するので、この攻撃に対し脆弱ではありません。X11UseLocalhost がデフォルト値 "yes" のままになっている場合も、脆弱ではありません。 移植版 OpenSSH 5.1 では、すべてのオペレーティング システムでこの問題を回避するために、X11UseLocalhost が no と設定された場合には、SO_REUSEADDR を設定しません この問題は 5.1 より前のバージョン 5.x および 5.1p1 において報告されています。		
参照	* CONFIRM: http://openssh.com/security.html * CONFIRM: http://www.openssh.com/ja/txt/release-5.1 * BID: 30339 http://www.securityfocus.com/bid/30339 * VUPEN: ADV-2008-2148 http://www.frsirt.com/english/advisories/2008/2148 * SECTRACK: 1020537 http://www.securitytracker.com/id?1020537 * SECUNIA: 31179 http://secunia.com/advisories/31179 * XF: openssh-x11forwarding-info-disclosure(43940) http://xforce.iss.net/xforce/xfdb/43940 * BUGTRAQ: http://marc.info/?l=openssh-unix-dev &m=121084611818460 &w=2		
対策	少なくとも、OpenSSH バージョン 5.1 にアップグレードしてください。 詳細については参照を確認ください。		
以下で検出: 157.19.104.107 - ポート: 22			
SSH の脆弱なﾊﾞｰｼﾞｮﾝ : OpenSSH_5.0 NetBSD_Secure_Shell-20080403-hpn13v1			

	PHP 'phar/tar.c' におけるヒープ バッファ オーバーフローの脆弱性 (CVE-2012-2386)	CVE id	CVE-2012-2386
		SecureScout id	13991
説明	PHP 5.3.14 未満および 5.4.4 未満の 5.4.x の phar 拡張の tar.c 内の phar_parse_tarfile 関数の整数オーバーフローにより、リモートの攻撃者がヒープベース バッファ オーバーフローを誘発する、細工された tar ファイルを用いて、サービス不能 (アプリケーション クラッシュ) を引き起こしたり、場合によっては任意のコードを実行する可能性があります。		

	PHP 'phar/tar.c' におけるヒープ バッファ オーバーフローの脆弱性 (CVE-2012-2386)	CVE id	CVE-2012-2386
		SecureScout id	13991
参照	* MLIST: [oss-security] 20120522 Re: CVE request: PHP Phar - arbitrary code execution http://openwall.com/lists/oss-security/2012/05/22/10 * MISC: http://0x1バイト.blogspot.com/2011/04/php-phar-extension-heap-overflow.html * CONFIRM: http://git.php.net/?p=php-src.git;a=commit;h=158d8a6b088662ce9d31e0c777c6ebe90efdc854 * CONFIRM: http://www.php.net/ChangeLog-5.php * CONFIRM: https://bugs.php.net/bug.php?id=61065 * CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=823594 * CONFIRM: http://support.apple.com/kb/HT5501?viewlocale=ja_JP * APPLE: APPLE-SA-2012-09-19-2 http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html * SUSE: SUSE-SU-2012:0840 http://lists.opensuse.org/opensuse-security-announce/2012-07/msg00003.html		
対策	バージョン 5.4.4 もしくはこれ以降に更新してください。 詳細については参照を確認ください。		
以下で検出: 157.19.104.107 - ポート: 80			
HTTP バナーは: Apache/2.2.17 (Unix) DAV/2 PHP/5.3.22 PHP 検出バージョン: 5.3.22			

	PHP 'rfc1867.c ' におけるディレクトリ トラバーサルの脆弱性 (CVE-2012-1172)	CVE id	CVE-2012-1172
		SecureScout id	19896
説明	PHP 5.4.0 未満の rfc1867.c のファイル アップロードの実装は、NAME 属性値内の不正な [(角括弧) 文字列を適切に処理しません。それにより、リモートの攻撃者が複数のファイルのアップロードの最中に、自身のファイル名制限を欠くスクリプトを利用して、サービス不能 (不正な $_FILES インデックス) を引き起こしたり、ディレクトリ トラバーサル攻撃を実行することが容易になります。		
参照	* MLIST: [oss-security] 20120313 Re: CVE request for PHP 5.3.x Corrupted $_FILES indices lead to security concern http://openwall.com/lists/oss-security/2012/03/13/4 * MISC: http://isisblogs.poly.edu/2011/08/11/php-not-properly-checking-params/ * MISC: https://bugs.php.net/bug.php?id=48597 * MISC: https://bugs.php.net/bug.php?id=49683 * MISC: https://nealpoole.com/blog/2011/10/directory-traversal-via-php-multi-file-uploads/ * MISC: https://students.mimuw.edu.pl/~ai292615/php_multipleupload_overwrite.pdf * CONFIRM:		

	PHP 'rfc1867.c' におけるディレクトリトラバーサルの脆弱性 (CVE-2012-1172)	CVE id	CVE-2012-1172
		SecureScout id	19896
	http://svn.php.net/viewvc/php/php-src/branches/PHP_5_4/main/rfc1867.c?r1=321664 &r2=321663 &pathrev=321664 * CONFIRM: http://svn.php.net/viewvc?view=revision &revision=321664 * CONFIRM: http://www.php.net/ChangeLog-5.php#5.4.0 * CONFIRM: https://bugs.php.net/bug.php?id=54374 * CONFIRM: https://bugs.php.net/bug.php?id=55500		
対策	バージョン 5.4.1 もしくはこれ以降に更新してください。 詳細については参照を確認ください。		
以下で検出: 157.19.104.107 - ポート: 80			
HTTP バナーは: Apache/2.2.17 (Unix) DAV/2 PHP/5.3.22 PHP 検出バージョン: 5.3.22			

	PHP における深い再帰への保護を行わない脆弱性	CVE id	CVE-2006-1549
		SecureScout id	17780
説明	PHP のバージョン 4.4.2 および 5.1.2 において、ローカル ユーザが、再帰関数を定義および実行することによって、クラッシュ（セグメンテーション障害）を引き起こす可能性があります。注意:それ以降のバージョンでも影響を受ける可能性があることが、信頼性のある第 3 機関から報告されています。 この脆弱性は、バージョン 4.4.x および 5.x において確認されています。 この問題の修正版はありません。		
参照	* BUGTRAQ: 20060409 function *() php/apache Crash PHP 4.4.2 and 5.1.2 http://www.securityfocus.com/archive/1/archive/1/430453/100/0/threaded * BUGTRAQ: 20060410 Re: function *() php/apache Crash PHP 4.4.2 and 5.1.2 http://www.securityfocus.com/archive/1/archive/1/430598/100/0/threaded * BUGTRAQ: 20060412 Re: function *() php/apache Crash PHP 4.4.2 and 5.1.2 http://www.securityfocus.com/archive/1/archive/1/430742/100/0/threaded * BUGTRAQ: 20060414 Re: Re: function *() php/apache Crash PHP 4.4.2 and 5.1.2 http://www.securityfocus.com/archive/1/archive/1/431018/100/0/threaded * SREASONRES: 20060408 function *() php/apache Crash PHP 4.4.2 and 5.1.2 http://securityreason.com/achievement_securityalert/35 * MISC: http://www.php-security.org/MOPB/MOPB-02-2007.html * FRSIRT: ADV-2006-1290 http://www.frsirt.com/english/advisories/2006/1290 * OSVDB: 24485 http://www.osvdb.org/24485 * SECTRACK: 1015880 http://securitytracker.com/id?1015880 * SREASON: 2312 http://securityreason.com/securityalert/2312 * SREASON: 676 http://securityreason.com/securityalert/676		

	PHP における深い再帰への保護を行わない脆弱性	CVE id	CVE-2006-1549
		SecureScout id	17780
	* XF: php-function-dos(25704) http://xforce.iss.net/xforce/xfdb/25704		
対策	現在のところ、この問題の修正版はありません。 詳細については参照を確認ください。		
以下で検出: 157.19.104.107 - ポート: 80			
HTTP バナーは: Apache/2.2.17 (Unix) DAV/2 PHP/5.3.22 PHP 検出バージョン: 5.3.22			

低リスク脆弱性

	Apache HTTP Server の mod_log_config におけるサービス不能の脆弱性 (CVE-2012-0021)	CVE id	CVE-2012-0021
		SecureScout id	19949
説明	Apache HTTP Server 2.2.17 から 2.2.21 の mod_log_config モジュールの mod_log_config.c 内の log_cookie 関数は、スレッド MPM が使用される際に、 %{}C フォーマット文字列を適切に処理しません。それにより、リモートの攻撃者が名前と値の双方が欠けているクッキーを用いてサービス不能 (デーモン クラッシュ) を引き起こす可能性があります。		
参照	* CONFIRM: http://httpd.apache.org/security/vulnerabilities_22.html * CONFIRM: http://svn.apache.org/viewvc?view=revision &revision=1227292 * CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=785065 * CONFIRM: https://issues.apache.org/bugzilla/show_bug.cgi?id=52256 * CONFIRM: http://www.oracle.com/technetwork/jp/topics/security/top-1709266-ja.html * HP: HPSBMU02786 http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03360041		
対策	Apache をバージョン 2.2.22 もしくはこれ以降に更新してください。 詳細については参照を確認ください。		
以下で検出: 157.19.104.107 - ポート: 80			
HTTP バナーは: Apache/2.2.17 (Unix) DAV/2 PHP/5.3.22			

	HTTP バナーの露出	CVE id	CVE-1999-0655
		SecureScout id	15025
説明	ターゲット ホストは、Web サーバの正確なバージョンを漏えいします。 これを攻撃者に利用されて、既知の脆弱性の悪用を試行される可能性があります。		
参照	* MISC: Read section 10.14 of RFC 1945 http://www.ietf.org/rfc/rfc1945.txt		
対策	サーバを変更 (可能な時はいつでも) してください: HTTP ヘッダーの中にフィールドが返されます。 RFC 1945 はコンフィギュレーション可能であることを提案しています。		
以下で検出: 157.19.104.107 - ポート: 80			
HTTP サーバ バージョン: Apache/2.2.17 (Unix) DAV/2 PHP/5.3.22			

	ICMP タイムスタンプ返信の脆弱性	CVE id	CVE-1999-0524
		SecureScout id	11010
説明	通常は、ホストは ICMP の返信によって ICMP タイムスタンプのリクエストに応答します。 それは、ネットワークを氾濫させるために使われる恐れがあります。		
参照	* NETVIGILANCE-VULNDB: 11010 http://descriptions.securescout.com/tc/11010 * NETVIGILANCE-VULNDB: 11011		

	ICMP タイムスタンプ返信の脆弱性	CVE id	CVE-1999-0524
		SecureScout id	11010
	http://descriptions.securescout.com/tc/11011 * MISC: http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&externalId=1434 * OSVDB: 95 http://www.osvdb.org/95 * XF: icmp-netmask(306) http://xforce.iss.net/xforce/xfdb/306 * XF: icmp-timestamp(322) http://xforce.iss.net/xforce/xfdb/322		
対策	ICMP リクエスト パケットに応答しないようホストを設定してください。 そのサービスが必要無ければ、ファイアウォールで ICMP タイムスタンプ パケットを阻止してください。		
以下で検出: 157.19.104.107			
発信ﾀｲﾑｽﾀﾝﾌﾟ: 01:42:21.000 受信ﾀｲﾑｽﾀﾝﾌﾟ: 01:42:22.205 送信ﾀｲﾑｽﾀﾝﾌﾟ: 01:42:22.205			

	OpenSSH Forced command 処理における情報漏洩の脆弱性 (CVE-2012-0814)	CVE id	CVE-2012-0814
		SecureScout id	12185
説明	OpenSSH 5.7 未満の sshd の auth-options.c 内の auth_parse_options 関数は、authorized_keys command オプションを含んだデバック メッセージを提供します。それにより、リモート認証されたユーザがこのメッセージを参照することで、機密性の高い可能性のある情報を潜在的に獲得する可能性があります。		
参照	* MLIST: [oss-security] 20120126 CVE Request: Debian (others?) openssh-server: Forced Command handling leaks private information to ssh clients http://openwall.com/lists/oss-security/2012/01/26/15 * MLIST: [oss-security] 20120126 Re: CVE Request: Debian (others?) openssh-server: Forced Command handling leaks private information to ssh clients http://openwall.com/lists/oss-security/2012/01/27/1 * MLIST: [oss-security] 20120126 Re: CVE Request: Debian (others?) openssh-server: Forced Command handling leaks private information to ssh clients http://openwall.com/lists/oss-security/2012/01/26/16 * MLIST: [oss-security] 20120127 Re: CVE Request: Debian (others?) openssh-server: Forced Command handling leaks private information to ssh clients http://openwall.com/lists/oss-security/2012/01/27/4 * CONFIRM: http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=657445 * CONFIRM: http://www.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/auth-options.c * CONFIRM: http://www.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/auth-options.c.diff?r1=1.53;r2=1.54 * BID: 51702 http://www.securityfocus.com/bid/51702 * OSVDB: 78706 http://osvdb.org/78706 * XF: opensshserver-commands-info-disc(72756)		

	OpenSSH Forced command 処理における情報漏洩の脆弱性 (CVE-2012-0814)	CVE id	CVE-2012-0814
		SecureScout id	12185
	http://xforce.iss.net/xforce/xfdb/72756		
対策	OpenSSH を少なくとも、バージョン 5.7 にアップグレードしてください。 詳細については参照を確認ください。		
以下で検出: 157.19.104.107 - ポート: 22			
SSH の脆弱なﾊﾞｰｼﾞｮﾝ : OpenSSH_5.0 NetBSD_Secure_Shell-20080403-hpn13v1			

	SSH サービスが稼動しています	CVE id	GENERIC-MAP-NOMATCH
		SecureScout id	13078
説明	サーバに接続して受信したバッファを処理することによって、 SSH サーバのタイプとバージョンが見つけられます。 この情報はネットワーク上で攻撃をしかけるために利用される恐れがあります。		
参照	* NETVIGILANCE: http://descriptions.securescout.com/tc/13078		
対策	ログインのバナーを変更し、公開される情報を制限してください。		
以下で検出: 157.19.104.107 - ポート: 22			
SSH-2.0-OPENSSH_5.0 NETBSD_SECURE_SHELL-20080403-HPN13V1			

	Traceroute が利用可能	CVE id	CVE-1999-0525
		SecureScout id	11100
説明	traceroute アプリケーションはホストまでのネットワーク経路をリスト表示します。これは、中間ルータの名称及び内部 IP のアドレッシング方式を含んだ、ルーティングパスについての情報を公開します。		
参照	* MISC: Traceroute http://en.wikipedia.org/wiki/Traceroute		
対策	Traceroute はインターネットに接続する全てのマシンで利用可能です。 インターナル ネットワークで用いられるマシンでは、不要な全 UDP ポートを外部からフィルタし、Traceroute はファイアウォールの内部から応答します。Traceroute リクエストは通常 32768 番以上の UDP ポートを使用します。Traceroute の応答は、ICMP プロトコル上の TTL 超過 -type 11- メッセージおよび ICMP プロトコル上のサービスが利用不能 -type 3- メッセージになる可能性があります。		
以下で検出: 157.19.104.107			
ﾎｽﾄ gateway107.csse.muroran-it.ac.jp への Traceroute : > 157.19.201.126 157.19.201.126 > gateway107.csse.muroran-it.ac.jp 157.19.104.107			