株式会社サンプルデータ御中

セキュリティ診断結果報告書

平成 25 年 9 月 1 日

株式会社アール・エヌ・エー

目次

1. 診断情報

診断実施日	平成 25 年 8 月 23 日～8 月 25 日
診断種別	ネットワーク診断、Web アプリケーション診断
ネットワーク診断 対象 IP アドレスと検出されたポート番号	184.22.200.108 (＊検出ポート番号無し) 163.43.160.153 (25/tcp) 121.83.238.249 (＊検出ポート番号無し) 182.48.42.245 (＊検出ポート番号無し) 49.212.178.34 (80/tcp、443/tcp) 95.170.83.216 (80/tcp、443/tcp) 163.43.164.245 (80/tcp) 163.43.165.1 (21/tcp、80/tcp、443/tcp) 211.8.18.40 (21/tcp、80/tcp) 163.43.163.179 (80/tcp、443/tcp) 49.212.200.252 (80/tcp) 163.43.163.40 (1723/tcp)
Web アプリケーション診断 対象 URL (ホスト名)	www.gax.jp custum.gax.jp erp.gax.jp order.gax.jp ssl.gax.jp ssl1.gax.jp ssl2.gax.jp ssl3.gax.jp

2. リスクのレベルと警告数

2.1 ネットワーク診断

IP アドレス	High(高)	Medium(中)	Low(低)	Info(情報)
184.22.200.108	0	0	0	0
163.43.160.153	0	0	0	3
121.83.238.249	0	0	0	0
182.48.42.245	0	0	0	0
49.212.178.34	0	3	0	7
95.170.83.216	0	2	0	6
163.43.164.245	0	3	0	5
163.43.165.1	0	2	1	0

211.8.18.40	1	3	1	4
163.43.163.179	0	2	0	0
49.212.200.252	0	2	0	0
163.43.163.40	0	0	0	0

2.2 Web アプリケーション診断

URL	High(高)	Medium(中)	Low(低)	Info(情報)
www.gax.jp	0	0	0	0
custum.gax.jp	0	0	0	0
erp.gax.jp	0	0	0	0
order.gax.jp	0	0	0	0
ssl.gax.jp	0	1	0	0
ssl1.gax.jp	0	0	0	0
ssl2.gax.jp	1	1	1	0
ssl3.gax.jp	0	0	0	0

3. 総評

今回の脆弱性診断では、ネットワーク診断、および Web アプリケーション診断を実施しました。
ネットワーク診断においては High(高)レベルの脆弱性として、HTTP サーバの Apache に関する脆弱性が検出されています。対策を施された Apache のバージョンがリリースされていますのでバージョンアップをお勧めします。
また、Web アプリケーション診断においては High（高）レベルの脆弱性として、SQL インジェクションが検出されています。クライアント側からのフォーム入力をチェックする仕組みを導入されることをお勧めします。

全体的にはネットワーク、および Web アプリケーション診断において 1 つずつ High（高）レベルの脆弱性が検出されましたが、その他大きな問題点はありませんでした。
今後も定期的に脆弱性診断、および対策を実施することでより、堅牢なシステムが維持されますので、継続的なメンテナンスをご検討下さい。

4. リスク詳細

4.1 ネットワーク診断結果

Apache HTTP サーバへの DoS 攻撃	
リスクレベル	High（高）
対象 IP	211.8.18.40
ポート番号	80/tcp
説明	Apache HTTP サーバは DoS 攻撃を受ける脆弱性があります。
参照	http://archives.neohapsis.com/archives/fulldisclosure/2011-08/0203.html http://www.gossamer-threads.com/lists/apache/dev/401638 http://www.nessus.org/u?404627ec http://httpd.apache.org/security/CVE-2011-3192.txt http://www.nessus.org/u?1538124a http://www-01.ibm.com/support/docview.wss?uid=swg24030863
対策	Apache httpd 2.2.21 以降へバージョンアップする。 ただし、 CentOS5 系は、httpd-2.2.3-53.el5 以降で対応済 CentOS6 系は、httpd-2.2.15-9.el6 以降で対応済

PHP expose_php 情報公開	
リスクレベル	Medium（中）
対象 IP	49.212.178.34 95.170.83.216 163.43.164.245
ポート番号	80/tcp、443/tcp
説明	特別な URL を指定することで、バージョンなどの PHP に関する情報を表示することができます。 URL 例： http://www.gax.jp/index.php/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000
参照	http://www.0php.com/php_easter_egg.php http://seclists.org/webappsec/2004/q4/324
対策	php.ini ファイルで expose_php=Off に設定する。

HTTP TRACE メソッド	
リスクレベル	Medium（中）
対象 IP	49.212.178.34 95.170.83.216 163.43.164.245 163.43.165.1 211.8.18.40 163.43.163.179 49.212.200.252
ポート番号	80/tcp、443/tcp
説明	デバッグ関数 HTTP TRACE メソッドが有効になっています。
参照	http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_eorder.pdf http://www.apacheweek.com/issues/03-01-24 http://www.kb.cert.org/vuls/id/288308 http://www.kb.cert.org/vuls/id/867593 http://download.oracle.com/sunalerts/1000718.1.html
対策	TRACE メソッドを無効化する。

Apache HTTP 情報公開	
リスクレベル	Medium（中）
対象 IP	49.212.178.34 163.43.164.245 211.8.18.40 163.43.163.179 49.212.200.252
ポート番号	80/tcp、443/tcp
説明	Apache の現在のバージョンは Apache に関する情報公開の脆弱性があります。
参照	http://fd.the-wildcat.de/apache_e36a9cf46c.php http://httpd.apache.org/security/vulnerabilities_22.html http://svn.apache.org/viewvc?view=revision&revision=1235454
対策	Apache httpd 2.2.22 以降へバージョンアップする。

Apache mod_status /server-status 情報公開	
リスクレベル	Medium（中）
対象 IP	163.43.165.1 211.8.18.40
ポート番号	80/tcp、443/tcp
説明	URL /server-status をリクエストすることにより、Apache に関する情報公開の脆弱性があります。
対策	不要であれば mod_status を無効化する。

FTP 認証情報の搾取	
リスクレベル	Low（低）
対象 IP	163.43.165.1 211.8.18.40
ポート番号	21/tcp
説明	FTP の認証情報が平文で送信されるため第三者に漏洩する可能性があります。
対策	SFTP (part of the SSH suite)、もしくは FTPS(FTP over SSL/TLS) に切替える。

TCP タイムスタンプ	
リスクレベル	Information（情報）
対象 IP	163.43.160.153 49.212.178.34 95.170.83.216 163.43.164.245 211.8.18.40
説明	TCP タイムスタンプ情報が含まれています。 サーバの稼働時間帯を確認することが出来ます。
参照	http://www.ietf.org/rfc/rfc1323.txt

FQDN 情報（逆引き）	
リスクレベル	Information（情報）
対象 IP	163.43.160.153 49.212.178.34 95.170.83.216 163.43.164.245 211.8.18.40
説明	対象サーバの FQDN 情報（逆引き）が確認できます。
備考	163.43.160.153 → 163.43.160.153.gax.jp 49.212.178.34 → www.gax.jp 95.170.83.216 → ssl1.gax.jp 163.43.164.245 → ssl2.gax.jp 211.8.18.40 → ssl3.gax.jp

OS 情報	
リスクレベル	Information（情報）
対象 IP	163.43.160.153 49.212.178.34 95.170.83.216 163.43.164.245 211.8.18.40
説明	対象サーバの OS 情報が確認できます。
備考	163.43.160.153 → Microsoft Windows Server 2003 49.212.178.34 → Linux Kernel 2.6 95.170.83.216 → Linux Kernel 2.6 163.43.164.245

	→ Linux Kernel2.6 211.8.18.40 → Linux Kernel2.4

バーチャルホスト名	
リスクレベル	Information（情報）
対象 IP	49.212.178.34 95.170.83.216 211.8.18.40
説明	バーチャルホスト名が検出されています。
参照	http://en.wikipedia.org/wiki/Virtual_hosting
備考	49.212.178.34 → yb.gax.jp 95.170.83.216 → asp.gax.jp 211.8.18.40 → www.gax.jp

ディレクトリ情報の列挙	
リスクレベル	Information（情報）
対象 IP	49.212.178.34 163.43.164.245
参照	http://projects.webappsec.org/Predictable-Resource-Location
説明	Web サーバ上のディレクトリ情報が搾取できます。
備考	49.212.178.34 → /admin, /css, /error, /images, /js 163.43.164.245 → /cgi-bin /error

HTTP Web サーバ名	
リスクレベル	Information（情報）
対象 IP	49.212.178.34 95.170.83.216 163.43.164.245
説明	Web サーバ名が搾取できます。
備考	Web サーバ名　Apache

SSL／TLS バージョン	
リスクレベル	Information（情報）
対象 IP	49.212.178.34 95.170.83.216
説明	SSL／TLS のバージョン情報が搾取できます。
参照	SSL／TLS バージョン SSLv3/TLSv1.0

4.2 Web アプリケーション診断結果

SQL インジェクション	
リスクレベル	High（高）
対象ホスト名	ssl2.gax.jp
説明	SQL インジェクションが可能になっています。入力されたパラメータはデータベース操作のための SQL クエリー として認識されます。
URL	https://ssl2.gax.jp/postcard/api/templates/find?
パラメータ	page=1&length=50&type=1 AND 1=1
URL	https://ssl2.gax.jp/postcard/api/templates/sequence?
パラメータ	type=1 AND 1=1&color_id=0&design_id=0&usefulness_id=0&number_id=0
URL	https://ssl2.gax.jp/10000_postcard/index/module/Deliver/action/¥ Set/sk/7439db6052c739629b28505753a1a92f/
パラメータ	rcpttel1front_sub=+AND+1%3D1
参照	The OWASP guide at http://www.owasp.org/documentation/guide http://www.sqlsecurity.com/DesktopDefault.aspx?tabid=23 http://www.spidynamics.com/whitepapers/WhitepaperSQLInjection.pdf
対策	クライアント側での確認があったとしても、クライアントの入力を信頼してはいけません。入力された文字列が想定されているパターンに合致しているかの確認をして下さい。

パスワードオートコンプリート	
リスクレベル	Medium（中）
対象ホスト名	ssl.gax.jp ssl2.gax.jp
説明	AUTOCOMPLETE 属性がパスワード入力を含むフォームの中で有効になっています。パスワードがブラウザに格納されるため、第三者に利用される可能性があります。
URL	https://ssl.gax.jp/mypage/login
Other Information	<input type="password" class="text" name="password" maxlength="8" value="">
URL	https://ssl2.gax.jp/10000_postcard/index/module/Login/action/AuthIndex¥ /sessid/
Other Information	<input type="password" name="password" value="" size="50" maxlength="8">
参照	http://msdn.microsoft.com/library/default.asp?url=/workshop/author/forms/autocomplete_ovr.asp
対策	AUTOCOMPLETE = OFF に設定する。

バックアップ、未使用ファイルの存在	
リスクレベル	Low（低）
対象ホスト名	ssl2.gax.jp
説明	バックアップファイルや使用されていないファイルが存在しています。
URL	対象ファイルの拡張子を以下に示します。 https://ssl2.gax.jp/postcard/js/views/***.js~ https://ssl2.gax.jp/postcard/js/views/***.bak https://ssl2.gax.jp/postcard/js/views/***.js.java https://ssl2.gax.jp/postcard/js/views/***.old https://ssl2.gax.jp/postcard/js/views/***.inc
対策	不要なファイルの場合は削除する。

サンプルはここまでです。