ご担当者様

セキュリティオプションをご利用いただき、ありがとうございます。

セキュリティ診断の結果をレポートとしてご用意いたしました。
ご利用サーバーのセキュリティ施策にお役立てください。

■診断スクリプトバージョン情報

バージョン：1.0.x
最新のバージョンをご利用です。

サーバーにインストールされている診断プログラムのバージョンを表示しています。

■サービス情報

ホストID：example.com

診断対象サーバーについて一意の識別子をホストIDとして表示しています。

■システム情報

ホスト名：example.com
IPアドレス：192.168.1.1
OS：CentOS Linux release 7.3.1611 (Core)
サーバー管理ツール：plesk
Pleskバージョン：plesk 17.8.11 CentOS 7 1708180920.15

OSバージョン、Pleskバージョンはサーバー内情報から取得します。

■診断実行日時

Tue Jan 5 21:12:01 JST 2021

診断実行前にdateコマンドを実行し、診断実行日時として表示しています。

■ルートキット検出ツールの実行結果

ルートキット自動検出ツールの実行結果です。
ルートキットとはコマンド改ざんによる不正アクセスの隠蔽、
バックドアの設置を行ったりするために、不正アクセスを行う
第三者によって使用されるツール群です。

「INFECTED」という表記は、コマンドの改竄を示しています。

システム改ざん、不正ツールを検知するオープンソースのツールchkrootkitを実行し、その結果を見やすいかたちで表示しています。

<組み込みコマンドの汚染状況>
su [not infected]
pstree [not infected]
telnetd [not found]
identd [not found]
:
:
cron [not infected]
vdir [not infected]
ldsopreload [not infected]
egrep [not infected]
sshd [not infected]
ifconfig [not infected]

<システム不正利用状況>
lkm [not infected]
asp [not infected]
sniffer [eth0: PF_PACKET(/usr/sbin/dhclient)]
z2 [not infected]
wted [not infected]
bindshell [not infected]
aliens ...details were reported as follows
>
> /usr/lib/debug/usr/.dwz
> /usr/lib/python2.7/site-packages/fail2ban/tests/files/config/apache-auth/basic/authz_owner/.htaccess
> /usr/lib/python2.7/site-packages/fail2ban/tests/files/config/apache-auth/basic/authz_owner/.htpasswd
> /usr/lib/python2.7/site-packages/fail2ban/tests/files/config/apache-auth/basic/file/.htaccess
> /usr/lib/python2.7/site-packages/fail2ban/tests/files/config/apache-auth/basic/file/.htpasswd
> /usr/lib/python2.7/site-packages/fail2ban/tests/files/config/apache-auth/digest/.htaccess
> /usr/lib/python2.7/site-packages/fail2ban/tests/files/config/apache-auth/digest/.htpasswd
> /usr/lib/python2.7/site-packages/fail2ban/tests/files/config/apache-auth/digest_anon/.htaccess
> /usr/lib/python2.7/site-packages/fail2ban/tests/files/config/apache-auth/digest_anon/.htpasswd
> /usr/lib/python2.7/site-packages/fail2ban/tests/files/config/apache-auth/digest_time/.htaccess
> /usr/lib/python2.7/site-packages/fail2ban/tests/files/config/apache-auth/digest_time/.htpasswd
> /usr/lib/python2.7/site-packages/fail2ban/tests/files/config/apache-auth/digest_wrongrelm/.htaccess
> /usr/lib/python2.7/site-packages/fail2ban/tests/files/config/apache-auth/digest_wrongrelm/.htpasswd
> /usr/lib/python2.7/site-packages/fail2ban/tests/files/config/apache-auth/noentry/.htaccess
> /usr/lib/mailman/.qmail

chkutmp [not infected]
slapper [not infected]
w55808 [not infected]

各項目の診断対象説明
w55808：ワームの一種
slapper：ワームの一種
asp：ワームの一種
lkm：LKM(Loadable Kernel Module)型ルートキット
sniffer：プロミスキャスモードによるネットワークの不正使用
chkutmp：診断時点のログイン情報改ざん(mingettyに対する警告は誤検出です。)
wted：ログイン履歴改ざん
z2：ログイン履歴改ざん
bindshell：不正なポート使用(「INFECTED(PORTS: 465)」は誤検出です。)
aliens：ネットワーク不正利用のログ、ルートキットの設定ファイル

■シェルアクセス可能なシステムアカウント

シェル(sh、bash等)の使用が許可されているアカウントを表示しています。

root
postgres
magicspam
vulsuser

/etc/passwdファイルでシェルの利用が許可されている
ユーザーを確認し、表示しています。

■ログイン履歴

サーバーにログインしたユーザーの履歴です。
接続元のIPアドレス、ユーザー名、接続した日時、接続方法(FTP,SSHなど)を表示しています。

IP-Address:192.168.0.1 Date:Wed Nov 11 11:39:39 2015 User:example1 Host:192.168.0.1 Type:FTP
IP-Address:192.168.0.1 Date:Wed Nov 11 01:54:07 2015 User:example1 Host:192.168.0.1 Type:FTP
IP-Address:192.168.0.1 Date:Wed Nov 11 01:53:34 2015 User:example1 Host:192.168.0.1 Type:FTP
IP-Address:192.168.0.1 Date:Fri Nov 6 12:46:39 2015 User:example1 Host:192.168.0.1 Type:FTP
・
・
・
IP-Address:192.168.0.2 Date:Thu Sep 17 19:22:18 2015 User:example2 Host:192.168.0.2 Type:SSH
IP-Address:192.168.0.2 Date:Mon Sep 14 11:07:30 2015 User:example2 Host:192.168.0.2 Type:SSH
IP-Address:192.168.0.2 Date:Mon Sep 14 10:27:11 2015 User:example2 Host:192.168.0.2 Type:SSH
IP-Address:0.0.0.0 Date:Fri Sep 11 15:20:03 2015 User:root Host: Type:ttyS0

SSH、FTPのログイン履歴を
/var/log/wtmpより取得し、
表示しています。

■失敗したSSH接続の履歴

SSH接続に失敗した記録です。
接続を試みた日時、使用されたユーザー名、接続元のIPアドレスを表示しています。
不正なIPアドレスからのアクセス記録が多数ある場合は、
TCPWrapper、ファイヤーウォールによるアクセス元制限をご検討ください。

Date:Jan 24 04:07:07 User:a IP-Address:x.x.x.x
Date:Jan 24 10:44:00 User:webmaster IP-Address:x.x.x.x
Date:Jan 24 10:44:03 User:postmaster IP-Address:x.x.x.x
Date:Jan 24 11:37:50 User:guest IP-Address:x.x.x.x
Date:Jan 24 11:39:28 User:info IP-Address:x.x.x.x
・
・
・
Date:Jan 24 14:04:57 User:admin IP-Address:x.x.x.x
Date:Jan 24 20:57:46 User:ADMIN IP-Address:x.x.x.x
Date:Jan 24 22:52:38 User:account IP-Address:x.x.x.x
Date:Jan 24 22:54:36 User:administrateur IP-Address:x.x.x.x
Date:Jan 24 23:21:40 User:Administrator IP-Address:x.x.x.x

/var/log/secureよりログインに失敗したSSH接続を表示しています。
TCPWrapper、ファイアーウォールによるアクセス元制限は
セキュリティオプション内で代行可能です。

■失敗したFTP接続の履歴

FTP接続に失敗した記録です。不正なIPアドレスからのアクセス記録が多数ある場合は、
接続を試みた日時、使用されたユーザー名、接続元のIPアドレスを表示しています。
TCPWrapper、ファイヤーウォールによるアクセス制限をご検討ください。

Date:Dec 27 17:39:57 User:admin IP-Address:x.x.x.x
Date:Jan 2 23:57:51 User:server IP-Address:x.x.x.x
Date:Jan 3 07:33:34 User:administrator IP-Address:x.x.x.x
Date:Jan 3 07:33:34 User:user IP-Address:x.x.x.x
Date:Jan 3 07:33:34 User:test IP-Address:x.x.x.x
・
・

/var/log/secureよりログインに失敗したSSH接続を表示しています。
TCPWrapper、ファイアーウォールによるアクセス元制限は
セキュリティオプション内で代行可能です。

・
Date:Jan 17 02:55:10 User:anonymous IP-Address:x.x.x.x
Date:Jan 17 07:20:49 User:ftp IP-Address:x.x.x.x
Date:Jan 18 00:10:22 User:login IP-Address:x.x.x.x
Date:Jan 20 10:36:40 User:anonymous IP-Address:x.x.x.x
Date:Jan 20 20:09:36 User:anonymous IP-Address:x.x.x.x

■メールパスワードの脆弱性(Pleskのみ)

安全性の低いパスワードが設定されたメールアドレスを表示しています。

例えば以下のような場合に安全性に問題があると診断されます。

・アカウント名と同じ文字列
・辞書に載っている単語が含まれている
・単純な並びの文字列(アルファベット順、数字順など)

info@example.com

OSのパスワード脆弱性チェック用ライブラリを使用して
Pleskのメールアカウントに設定されたパスワードをテストし、
安全でないパスワードが設定されているメールアカウントを
表示します。

■YUMアップデートリスト

インストールされているソフトウェアのうち更新パッケージが提供されているものの一覧を表示しています。

GeoIP.x86_64:1.5.0-14.el7:base
GeoIP-devel.x86_64:1.5.0-14.el7:base
ImageMagick.x86_64:6.9.10.68-4.el7:updates
ImageMagick-devel.x86_64:6.9.10.68-4.el7:updates
NetworkManager.x86_64:1.18.8-2.el7_9:updates
NetworkManager-libnm.x86_64:1.18.8-2.el7_9:updates
NetworkManager-team.x86_64:1.18.8-2.el7_9:updates
:
:
virt-what.x86_64:1.18-4.el7:base
wget.x86_64:1.14-18.el7_6.1:base
wpa_supplicant.x86_64:2.6-12.el7:base
xfsdump.x86_64:3.1.7-1.el7:base
xfsprogs.x86_64:4.5.0-22.el7:base
xinetd.x86_64:2.3.15-14.el7:base
xorg-x11-font-utils.x86_64:7.5-21.el7:base
xorg-x11-proto-devel.noarch:2018.4-1.el7:base
yum.noarch:3.4.3-168.el7.centos:base
yum-plugin-fastestmirror.noarch:1.1.31-54.el7_8:base
zlib.x86_64:1.2.7-18.el7:base
zlib-devel.x86_64:1.2.7-18.el7:base
----

yum check-updateで更新パッケージがあるものを列挙しています。

オープンソースのツールVulsによる脆弱性診断
を実行し、その結果を見やすいかたちで表示し
ています。

■脆弱性チェックの結果

脆弱性概要 : GNU Libtasn1 の asn1_der_decoding には、スタックベースのバッファオーバーフローの脆弱性が存在します。
CVE番号　: CVE-2015-2806
詳細URL　: https://jvndb.jvn.jp/ja/contents/2015/JVNDB-2015-002209.html

脆弱性概要 : Heap-based buffer overflow in dnsmasq before 2.78 allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted DNS response.
CVE番号　: CVE-2017-14491
詳細URL　: https://access.redhat.com/security/cve/CVE-2017-14491

脆弱性概要 : procmail には、バッファエラーの脆弱性が存在します。
CVE番号　: CVE-2017-16844
詳細URL　: https://jvndb.jvn.jp/ja/contents/2017/JVNDB-2017-010248.html

脆弱性概要 : Linux Kernel には、解放済みメモリの使用に関する脆弱性が存在します。
CVE番号　: CVE-2017-18017
詳細URL　: https://jvndb.jvn.jp/ja/contents/2017/JVNDB-2017-011875.html

:
:

脆弱性概要 : Systems with microprocessors utilizing speculative execution and address translations may allow unauthorized disclosure of information residing in the L1 data cache to an attacker with local user access with guest OS privilege via a terminal page fault and a side-channel analysis.
CVE番号　: CVE-2018-3646
詳細URL　: https://access.redhat.com/security/cve/CVE-2018-3646

脆弱性概要 : Systems with microprocessors utilizing speculative execution and branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis.
CVE番号　: CVE-2017-5753
詳細URL　: https://access.redhat.com/security/cve/CVE-2017-5753

脆弱性概要 : Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis of the data cache.
CVE番号　: CVE-2017-5754
詳細URL　: https://access.redhat.com/security/cve/CVE-2017-5754

脆弱性概要 : The VFIO PCI driver in the Linux kernel through 5.6.13 mishandles attempts to access disabled memory space.
CVE番号　: CVE-2020-12888
詳細URL　: https://access.redhat.com/security/cve/CVE-2020-12888

[セキュリティ関連の参考情報]

〇最近の脆弱性情報(情報提供元:情報処理推進機構)

この情報は情報処理推進機構(IPA)が提供する脆弱性対策情報データベース(JVN iPedia)より、

・Linuxカーネル及びLinuxOSを構成する各種ソフトウェアツール
・Redhat Enterprise Linux、CentOS
・Apache、MySQL、PHP、Postfix等Linuxサーバーで一般的に利用されるミドルウェア
・phpMyAdmin、WordPress等Linuxサーバーで一般的に利用されるアプリケーション

にかかわる脆弱性情報をMyJVN APIを利用して自動取得しています。

Apache Struts 2 において任意のコードが実行可能な脆弱性 (S2-061)
https://jvndb.jvn.jp/ja/contents/2020/JVNDB-2020-000084.html

※過去1ヶ月に発見された影響度の高いものをAPIにより取得し表示しています。
※本情報は情報処理推進機構により公開されている情報となり、ご利用サーバーに存在する脆弱性を検知した結果ではございませんので、ご注意ください。

過去1カ月以内に発見された
緊急度の高い脆弱性情報を表示しています。

このメールは、レポートシステムより自動的に送信されています。
返信は受け付けておりませんのでご了承ください。

レポートの内容について、ご不明な点がございましたら、
サポートセンターまでお問い合わせください。

・メールでのお問い合わせ
お問合せフォーム: フォームURL
・電話でのお問い合せ
Tel: サポート窓口電話番号

GMOクラウド お客さまサービスセンター
〒150-8512 東京都渋谷区桜丘町26-1 セルリアンタワー