e-securIT

[Configurer la sécurité dans Sendmail]

http://securit.free.fr

[securIT@free.fr]

TABLE DES MATIÈRES

1. INSTALLER SENDMAIL

1.1. VERSION DE SENDMAIL

Sendmail est un programme complexe qui a laissé apparaître, au cours de ces nombreuses années d'utilisation, beaucoup de failles de sécurité. Il est donc essentiel de toujours utiliser des versions récentes de Sendmail, éliminant ainsi le risque de compromission par l'exploitation d'une faille ancienne.

Les dernières versions de Sendmail sont disponibles directement sur le site Web :

ftp://ftp.sendmail.org/pub/sendmail

A ce jour, il convient d'utiliser la version 8.11.2 de Sendmail :

ftp://ftp.sendmail.org/pub/sendmail/sendmail.8.11.2.tar.gz

1.2. INSTALLATION DE SENDMAIL

Pour installer Sendmail, se référer au guide d'installation.

Si Sendmail est installé sur une distribution Redhat 6.2 ou ultérieure (voire Mandrake), se référer au chapitre "Linux Sendmail Server" du très bon document "Securing and optimizing Redhat Linux 1.3" de Gerhard Mourani :

http://securit.free.fr/ressources/Securing-Optimizing-Linux-RH-Edition-1_3.pdf.

2. CONFIGURER LA SÉCURITÉ DE SENDMAIL

2.1. PERMISSIONS SUR LES FICHIERS SENDMAIL

Les permissions sur les différents fichiers utilisés par Sendmail doivent être étudiées avec attention. La plupart d'entre eux doit appartenir à root qui doit être le seul à disposer de droits en écriture sur ces fichiers.

Par exemple, sur un système Linux, on préconise les droits suivants :

CHEMIN-FICHIER	NATURE	PROPRIÉTAIRE	PERMISSIONS	
/usr/sbin/sendmail	Fichier	root	06511	-r-s--s--x
/etc/sendmail.cf	Fichier	root	0644 (ou 640)	-rw-r--r--
/etc/aliases	Fichier	root	0644	-rw-r--r--
/etc/aliases.db	Fichier	root	0644	-rw-r--r--
/etc/mail/mailertable	Fichier	root	0644	-rw-r--r--
/ec/mail/mailertable.db	Fichier	root	0644	-rw-r--r--
/var/spool/mqueue	Répertoire	root	0700	drwx------

Tableau n°1 : Permissions sur les fichiers/répertoires de Sendmail.

2.2. COMMANDES SENDMAIL

De nombreuses commandes SMTP dévoilent des informations sensibles sur la configuration de Sendmail et doivent être interdites.

2.2.1. Commandes wiz, kill, debug

Dans les versions récentes de Sendmail, les commandes wiz, kill et debug sont automatiquement interdites.

Pour vérifier si votre système supporte ou non ces commandes (et toute commande SMTP en général), il suffit d'effectuer un telnet sur le port 25 de la machine supportant Sendmail et, une fois connecté, entrer l'une des commandes :

debug

- Un message "500 Command unrecognised" certifie que votre système ne permet pas ces commandes.
- Un autre message (ex. : "200 Debug set") prouve que votre système supporte ces commandes. Il faut alors rapidement mettre à jour la version de Sendmail utilisée ou recompiler Sendmail en annulant ces commandes.

2.2.2. Cas des commandes debug et showq

La commande debug (mise en oeuvre lorsque la variable SMTPDEBUG est définie dans le fichier *Makefile* de Sendmail) permet aux développeurs de contrôler l'exécution du programme. Lorsque la commande debug est autorisée, la commande SMTP showq permet alors de regarder le contenu de la queue des messages. Il convient donc de ne jamais définir la variable SMTPDEBUG.

2.2.3. *Commandes vrfy, expn, finger*

Les commandes SMTP vrfy, finger et expn sont des commandes classiquement interdites car elles fournissent des informations sur les adresses de messagerie disponibles sur le serveur :

- La commande vrfy (verify) permet de tester l'existence d'une adresse de messagerie sur le serveur.
  Si la commande est supportée, on obtient les informations suivantes :

  vrfy victor
  250 Victor Hugo victor.hugo@domaine.fr
  vrfy toto
  550 toto... user unknown

  Si la commande n'est pas supportée :

  vrfy toto
  252 Cannot VRFY user; try RCPT to attempt delivery (or try finger)
  finger toto
  500 Command unrecognized: "finger toto"

- La commande expn (expand) est une extension de vrfy et permet de lister l'ensemble des adresses, les destinataires contenus dans les mailing-lists, les alias...
  Si la commande est supportée :

  expn all
  250 Victor Hugo victor.hugo@domaine.fr
  250 Emile Zola emile.zola@domaine.fr
  ...

  Si la commande n'est pas supportée :

  expn all
  502 Sorry, we do not allow this operation

Ces commandes, lorsqu'elles sont autorisées, dévoilent des informations qui peuvent être utilisés par une personne malveillante pour envoyer des messages non-sollicités (*spam*) ou tenter de découvrir le mot de passe associé au compte de messagerie.

Dans les versions récentes de Sendmail, ces commandes SMTP ne sont pas autorisées.

2.2.4. Restriction d'accès à la queue de messages

Il est nécessaire d'empêcher les utilisateurs non-membres du groupe auquel appartient la queue de messages de pouvoir lister le contenu de cette queue. Pour cela, il convient de spécifier l'option "restrictmailq".

2.2.5. Forcer l'identification du client

Il est possible de forcer Sendmail à demander à chaque client se connectant de s'identifier à l'aide de la commande HELO avant de pouvoir émettre un message. Pour cela, il convient de spécifier l'option "needmailhelo".

2.2.6. Configuration de Sendmail pour la sécurité des commandes SMTP

Pour interdire les commandes expn et vrfy, restreindre l'accès à la queue de messages et forcer l'identification du client, ajouter la ligne suivante dans /etc/sendmail.mc :

define('confPRIVACY_FLAGS', authwarnings novrfy noexpn restrictmailq neddmailhelo)

Une fois le fichier /etc/sendmail.mc ainsi modifié il convient de générer le nouveau fichier de configuration de Sendmail :

m4 /etc/sendmail.mc > /etc/sendmail.cf

Puis relancer le démon avec ce nouveau fichier de configuration :

/etc/rc.d/init.d/sendmail restart

2.3. AUTRES COMMANDES VULNÉRABLES

Deux autres failles de sécurité connues doivent être corrigées : les commandes OW et decode.

2.3.1. Commande OW

Une vulnérabilité connue de Sendmail consiste à accepter le "wizard's password". Ceci a lieu lorsque le fichier de configuration /etc/sendmail.cf contient une ligne avec OW différente de OW*. Un simple grep permet de vérifier cela :

more /etc/sendmail.cf | grep OW

Si la réponse n'est pas OW*, alors remplacer la ligne par OW*.

2.3.2. Commande decode

Une autre vulnérabilité connue consiste à laisser un alias decode dans le fichier /etc/aliases. Plus généralement, il est conseillé d'étudier tout alias redirigeant vers un programme et non un compte de messagerie).

Pour decode, ceci apparaît sous la forme suivante :

decode: "|/usr/bin/uudecode"

Deux possibilités peuvent être mises en œuvre :

- Enlever la ligne contenant decode.
- Remplacer la ligne contenant decode par :

decode: root

Ceci enverra un message à la boîte root lorsque quelqu'un tentera d'exploiter les failles liées à decode.

2.4. MESSAGE D'INVITE DE SENDMAIL

Par défaut, Sendmail envoie un certain nombre d'information lorsque l'on se connecte sur le serveur de messagerie :

telnet localhost 25
220-mail.domaine.fr ESMTP Sendmail 8.9.3/8.8.7 Tue, 20 Feb 2001 23:30:58 +0100

Ces informations permettent de découvrir sans effort la version de Sendmail utilisée (ici 8.9.3) ainsi que la version du fichier sendmail.cf (ici 8.8.7).

Pour éviter cela, il convient d'éliminer les options $v et $Z du fichier /etc/sendmail.mc :

define('confSMTP_LOGIN_MSG',$j Sendmail; $b)

2.5. LUTTER CONTRE LE SPAM

Le Spam correspond à du courrier électronique non-sollicité qui inonde en général les boîtes à lettre de manière illicite. En particulier, les spammers utilisent 3 moyens classiques pour tenter de découvrir les adresses de messagerie d'un domaine :

- Exécution des commandes EXPN et VRFY, d'où l'intérêt de désactiver ces commandes (cf. II.2.).
- Récupération d'adresses électroniques précisées sur des sites Web.
- Récupération d'adresses électroniques de participants à des forums de discussion (newsgroups).

2.5.1. Relayage de Spam

Le Spam s'est énormément développé grâce aux possibilités de relayage des serveurs de messagerie.

Depuis la version 8.9, Sendmail ne permet plus (par défaut) de relayer des messages : il est nécessaire que l'émetteur ou l'un des récepteurs du message appartienne au domaine géré par Sendmail.

En outre, Sendmail est capable de vérifier que le domaine d'appartenance de l'émetteur existe réellement (requête DNSlookup), mais ne permet pas de contrôler que la machine émettrice dispose bien d'une adresse IP du domaine résolu.

2.5.2. Realtime Blackhole List

Cette liste, disponible et maintenue par MAPS - http://maps.vix.com/, recense les spammers et les sites générant des spams. Sendmail dispose d'une option permettant d'interroger directement cette liste pour contrôler les messages reçus.

Ceci s'effectue en ajoutant la ligne suivante dans /etc/sendmail.mc :

FEATURE('rbl')

2.6. CONTRÔLER LE RELAYAGE AVEC SENDMAIL

2.6.1. Principes

Par défaut, le relayage est désactivé sur un serveur Sendmail, mais il peut être intéressant de l'activer de manière contrôlée dans certains cas (ne serait-ce que dans le cas très courant où Sendmail est utilisé en relais pour un domaine).

Pour ce faire, Sendmail fournit des moyens évolués permettant de contrôler et sécuriser le relayage, en évitant de devenir relais pour tous les messages.

Pour permettre le relayage sur le domaine, il convient de modifier le fichier /etc/sendmail.mc :

FEATURE('relay_entire_domain')

Puis générer le nouveau fichier de configuration et relancer le service.

On peut alors configurer le comportement de Sendmail en relais dans le fichier /etc/mail/access. Toute modification effectuée sur ce fichier est prise en compte par Sendmail lorsque l'administrateur exécute les commandes suivantes :

makemap hash /etc/mail/access < /etc/mail/access
/etc/rc.d/init.d/sendmail restart

Le fichier /etc/mail/access est constitué de deux colonnes :

- La première précise l'adresse SMTP, le nom de domaine, un nom de machine ou une adresse IP (éventuellement partielle).
- La deuxième colonne précise l'action effectuée :
  - OK : Sendmail accepte le message.
  - RELAY : Sendmail accepte le message et le relaye vers un autre serveur.
  - REJECT : Sendmail rejète le message avec un message d'avertissement.
  - DISCARD : Sendmail rejète le message directement.
  - Texte : Code d'erreur (compatible avec le RFC 821[1]).

2.6.2. Exemple d'implémentation

Considérons le cas d'école suivant : vous disposez d'un relais de messagerie Sendmail et vous désirez :

- Relayer tous les messages de votre domaine : domaine.fr.
- Rejeter tous les messages de votre concurrent commercial : concurrent.fr.
- Accepter les messages en provenance du directeur de votre concurrent commercial : directeur@concurrent.fr.
- Rejeter tous les messages en provenance d'un spammer identifié : spammer@hotmail.com.
- Rejeter tous les messages présentant une adresse de RFC 1918[2], par exemple : 192.168.0.0/16.

[1] RFC 821 : http://www.ietf.org/rfc/rfc821.

[2] RFC 1918 : http://www.ietf.org/rfc/rfc1918.

Le fichier /etc/mail/access doit avoir le contenu suivant :

spammer@hotmail.com	REJECT
192.168	REJECT
directeur@concurrent.fr	OK
concurrent.fr	550 Nous ne dialoguons pas avec nos concurrents !
domaine.fr	RELAY

A partir de la version 8.10 de Sendmail, il est possible d'ajouter des commandes spécifiques concernant les émetteurs (*left hand side*) pour une plus grande granularité du filtrage :

- Connect : traite les informations de connexion (client_name, client_address).
- From : filtrage sur le champ From de l'enveloppe.
- To : filtrage sur le champ To de l'enveloppe.

Soit, en reprenant l'exemple précédent :

From:spammer@hotmail.com	REJECT
Connect:192.168	REJECT
From:directeur@concurrent.fr	OK
From:concurrent.fr	550 Nous ne dialoguons pas avec nos concurrents !
From:domaine.fr	RELAY

2.7. FILTRER DES MESSAGES AVEC SENDMAIL

2.7.1. Filtrer les messages entrants

Sendmail offre des possibilités de filtrage de messages entrants en fonction de leur contenu. L'exemple classique (que l'on peut retrouvé sur le site de Sendmail.net[3]) concerne le ver LoveLetter présentant les caractéristiques suivantes :

Subject:ILOVEYOU
Body:kindly check the attached LOVELETTER coming from me.

Pour filtrer ce message en entrée, il convient de modifier le fichier /etc/sendmail.mc (puis mettre à jour le fichier /etc/sendmail.cf) :

```
LOCAL_RULESETS
# Love Letter worm checking routine.
# You just need enough of a pattern to match.
# Instructional note: Follow these instructions exactly.
# The format for the rule is
#
# RExactly the thing you want to quote
#
# No quote marks, no tabs, absolutely nothing in
# parentheses (like this, they're considered comments
# and will be removed before they get to the rules).
# After that, include the exact thing you want
# to quote, then a tab, and then the $#error.
# Note: The $* matches anything, so it's useful for
# wildcarding. This also scans all messages with
# Subject: headers and invokes a rule, so there is
# a performance hit.

HSubject: $>Check_Subject
D{MPat}ILOVEYOU
D{MMsg}This message may contain the LoveLetter virus.

SCheck_Subject
R${MPat} $*[tabulation]$#error $: 550 ${MMsg}
RRe: ${MPat} $*[tabulation]$#error $: 550 ${MMsg}
```

Remarque : le champ [tabulation] doit être remplacé par une véritable tabulation !

[3] http://sendmail.net/lovefix.shtml.

2.7.2. Filtrage des destinataires

Sendmail offre une possibilité supplémentaire de contrôler et filtrer les destinataires des messages. Ceci s'effectue en précisant dans le fichier /etc/sendmail.mc :

FEATURE('blacklist_recipients')

On peut alors modifier le fichier /etc/mail/access afin d'y préciser les adresses de messagerie ou serveurs qui ne pourront pas recevoir de messages. Par exemple :

- Victor Hugo étant mort, il ne peut plus recevoir de messages ☺.
- test.domaine.fr est un serveur Sendmail de tests interne, il ne doit pas être joint depuis l'extérieur.

Le fichier /etc/mail/access doit avoir le contenu suivant :

victor	550 Victor Hugo aura du mal à vous répondre !
Test.domaine.fr	REJECT

2.8. CONTRÔLER LES CONNEXIONS SMTP AVEC TCP WRAPPERS

TCP Wrappers[4] est le célèbre paquetage édité et maintenu par Wietse Venema permettant d'effectuer un contrôle et un filtrage au niveau réseau des connexions faites sur un système. Il est donc possible de contrôler les connexions par adresse IP, nom de machine ou nom de domaine.

Avant la version 8.8 de Sendmail, il était nécessaire d'exécuter Sendmail via Inetd et non comme démon afin de pouvoir bénéficier des services de TCP Wrappers.

Depuis la version 8.8, TCP Wrappers est supporté directement par Sendmail. Il est ainsi possible d'utiliser les fichiers /etc/hosts.allow et /etc/hosts.deny pour autoriser ou non les connexions au serveur de messagerie.

Pour des questions de sécurité, le fichier /etc/hosts.deny doit toujours contenir par défaut :

ALL:ALL

Ce qui signifie que tout ce qui n'est pas explicitement autorisé dans /etc/hosts.allow est interdit.

Attention : toujours laisser cependant un accès en administration distante sécurisée (ex. : avec SSH).

Si l'on souhaite autoriser tout serveur à communiquer avec un Sendmail local, sauf la machine spammer.vilain.fr, il convient d'effectuer les modifications suivantes :

- Dans /etc/hosts.allow :

  sendmail:ALL

- Dans /etc/hosts.deny :

  sendmail:spammer.vilain.fr
  ALL:ALL

[4] TCP Wrappers : http://securit.free.fr/tools/unix/nettools/tcp_wrappers.

2.9. ÉLIMINER LES ENTÊTES AVEC SENDMAIL

Il arrive souvent, notamment lorsque l'on souhaite utiliser Sendmail en tant que relais pour les messages sortants, de vouloir éliminer certains en-têtes des messages émis depuis des serveurs internes pour éviter de dévoiler à l'extérieur la topologie du système d'information.

Pour cela, il faut configurer Sendmail pour qu'il efface certains en-têtes des messages sortants :

- Modifier la configuration du fichier source conf.c.
- Recompiler Sendmail.
- Modifier le fichier sendmail.cf.

L'opération étant relativement complexe, elle n'est pas encore détaillée ici. Cependant, vous pouvez suivre le lien vers la page de Erin Jones[5] qui traite du sujet et propose une procédure intéressante.

2.10. CONFIGURER SENDMAIL POUR LUTTER CONTRE LES ATTAQUES DE DÉNI DE SERVICE

De nombreux de paramètres peuvent être configurés dans le fichier /etc/sendmail.mc afin d'offrir une résistance plus importante aux attaques visant à saturer les ressources du système.

Il est donc intéressant de fixer les variables suivantes dans le fichier /etc/sendmail.mc :

VARIABLES DU FICHIERS /etc/sendmail.mc	SIGNIFICATION
define('confMIN_FREE_BLOCKS','100')	Nb. minimum de bloques libres dans la queue pour accepter de nouveaux messages
define('confMAX_MESSAGE_SIZE','5000000')	Taille maximale des messages acceptés (en bits)
define('confAUTO_REBUILD','False')	Recompilation automatique des alias
define('confQUEUE_LA,'10')	Valeur : 8*nb_processeurs
define('confREFUSE_LA','8')	Valeur : 12*nb_processeurs
define('confMAX_DAEMON_CHILDREN','40')	Nb. max de processus fils autorisés par le démon Sendmail (par défaut : infini ; 40 pour 128 MB RAM). Au-delà, les connexions sont refusées. Attention : fixer cette variable peut constituer une source de déni de service !
define('confMAX_HEADERS_LENGTH','64')	Taille maximale de la somme des en-têtes
define('confMAX_MIME_HEADER_LENGTH','1024')	Taille maximale de certaines valeurs dans les en-têtes MIME
define('confMAX_RCPTS_PER_MESSAGE','100')	Nombre maximal de destinataires d'un message (par défaut : infini). Si ce nombre est dépassé, les destinateurs suivants reçoivent un code d'erreur 452 et la livraison du message est effectuée à la prochaine connexion.

Tableau n°2 : Paramétrage de sendmail.mc contre les dénis de service.

[5] HOWTO: use Sendmail 8.9.3 as a Mailhub to Strip Headers - http://erinjones.org/strip_headers.htm.

2.11. AJOUTER UNE MENTION LÉGALE AUX MESSAGES SORTANTS

Beaucoup d'entreprises souhaitent systématiquement ajouter une mention légale à l'ensemble des messages sortants, afin de se dégager de toute responsabilité en cas de problème. Ces messages prennent souvent la forme suivante :

> ----------
> Ce message et les éventuelles pièces jointes sont confidentiels ou appartenant à Nom_Entreprise et établis à l'intention exclusive de ses destinataires.
> Toute divulgation, utilisation, diffusion ou reproduction (totale ou partielle) non-autorisée de ce message, ou des informations qu'il contient, est interdite.
> Tout message électronique est susceptible d'altération. Nom_Entreprise décline toute responsabilité au titre de ce message s'il a été modifié ou falsifié.
> ----
> This e-mail and any attachments contain confidential information belonging to Nom_Entreprise and are intended solely for the addressees.
> Any unauthorised disclosure, use, dissemination or copying (either whole or partial) of this e-mail, or any information it contains, is prohibited.
> E-mails are susceptible to alteration. Neither Nom_Entreprise shall be liable for the message if altered or falsified.
> ----------

Sendmail ne permet pas simplement d'effectuer ce type d'opération, notamment à cause du problème du traitement des messages de type multimédia (MIME).

Certains développements spécifiques permettent cependant de résoudre une grande partie du problème, sur la base du travail de Al Smith (libmilter)[6].

Pour plus d'informations et pour obtenir les sources d'une solution proposée par Wouter Wijker sous RedHat 6.2 et Sendmail 8.11.1, contacter securit@free.fr.

2.12. EXPLOITATION DES MESSAGES DE LOGS

Sendmail peut générer énormément d'informations via le serveur syslog. La criticité des informations générant une alerte dans le syslog est fixée par la variable LogLevel dans /etc/mail/sendmail.cf.

Pour vérifier la valeur de LogLevel, exécuter la commande suivante (sous Linux) :

grep LogLevel /etc/mail/sendmail.cf
0 LogLevel=9

(par défaut, LogLevel est fixé à 9)

Le serveur syslog doit être configuré pour stocker les informations de logs dans un répertoire particulier.

Par exemple, sous Linux, syslog stocke ces informations dans /var/log/maillog.

Pour traiter les informations générées par Sendmail dans syslog, il existe des scripts Perl permettant de synthétiser ces informations. Pour cela, se reporter à la FAQ Sendmail-Section4-Q4.7 - http://www.sendmail.org/faq/section4.html#4.7.

[6] http://aeschi.ch.eu.org/milter.

3. RÉFÉRENCES

Quelques références intéressantes sur le même sujet :

- "Sendmail, 2nd edition" - Edition O'Reilly, janvier 1997, Bryan Costales & Eric Allman (ISBN 1-56592-222-0).
- "Secure any sendmail installation" http://sendmail.net/?feed=000705securitygeneral.
- "Securing Sendmail on 4 types of systems" http://sendmail.net/?feed=000710securitytaxonomy.
- "Securing and optimizing Redhat Linux 1.3" - Gerhard Mourani (ISBN 0-9700330-0-1) http://securit.free.fr/ressources/Securing-Optimizing-Linux-RH-Edition-1_3.pdf.
- "Anti-spam configuration control" - http://www.sendmail.org/m4/anti-spam.html.
- RFC 2505 - "Anti-Spam Recommandations for SMTP MTAs" - http://www.ietf.org/rfc/rfc2505.
- Forums : comp.mail.sendmail.

*****
***
*