Caoutchouc plein de malice

Julien Sterckeman

8 juin 2009

Formats dangereux

De nos jours, il n'est plus possible d'utiliser sans danger :

- des fichiers MS Office ;
- des fichiers OpenOffice ;
- des fichiers PDF.

Il ne reste donc plus que LaTeX.

Exécution du code malveillant

Distribution de code LaTeX malveillant par ingénierie sociale *via* :

- un fichier `.tex` à faire compiler ;
- un paquet `.sty` ;
- un modèle `.cls`.

Utilisation des points d'accroche (*hooks*) (`\everypar`, `\everyvbox`, *etc.*) ou de la commande `\AtBeginDocument`.

Penser malveillant

- techniques d'évasion
- fuite d'information
- déni de service
- exécution de code
- *egg dropping*

Techniques d'évasion (1/2)

```
\def\@startsection#1#2#3#4#5#6{%
\if@noskipsec \leavevmode \fi \par
\@tempskipa #4\relax \@afterindenttrue
\ifdim \@tempskipa <\z@
\@tempskipa -\@tempskipa \@afterindentfalse
\fi \if@nobreak \everypar{} \else
\addpenalty\@secpenalty\addvspace\@tempskipa
\fi
```

Vraiment besoin d'offuscation et d'évasion ?

Techniques d'évasion (2/2)

- création de macros (`\def`) ;
- modification du caractère d'échappement ;
- ajout de NOP (`\relax`).

⇒ Détection de motifs difficile...

```
\def\changepipe#1{\catcode`|=#1}
\changepipe0\relax|relax
|textbf{test}\relax
\changepipe12\relax
```

Fuite d'information

Lire un fichier :

- primitives TEX `\openin` et `\read` ;
- configuration par défaut sous Debian (`/etc/texmf/texmf.d/95NonPath.cnf`) : "`openin_any = a`" (all).

$\Rightarrow$ il est possible de lire n'importe quel fichier accessible à l'utilisateur.

Démo : fichier cls malveillant qui ajoute le contenu du fichier `/etc/passwd` à l'insu de l'utilisateur.

Déni de service

Écrire dans un fichier :

- primitives TEX `\openout` et `\write` ;
- configuration par défaut sous Debian : "`openout_any = p`" (paranoid).

⇒ on peut créer plein de fichiers dans le répertoire de compilation (LATEX B^{0}M$_B$).

Démo : fichier cls malveillant qui crée 1000 fichiers à la compilation.

Exécution de code

Exécuter une commande système :

- primitive TEX `\write18` ;
- configuration par défaut sous Debian : "`shell_escape = f`" (false).

⇒ on ne peut pas exécuter directement de commandes système à la compilation avec `pdflatex`, par défaut.

Egg dropping (1/2)

- `openout_any = p`, donc :
  - on ne peut pas écrire dans un répertoire parent,
  - le nom de fichier ne peut pas commencer par `.` (`.bashrc`, *etc.*) ;
- la plupart des implémentations ajoutent l'extension `.tex` si le nom de fichier n'en possède pas (`Makefile`).

$\Rightarrow$ pas de réécriture évidente possible de scripts ou fichiers de configuration.

Egg dropping (2/2)

Idées :

- générer un PDF exploitant une vulnérabilité JavaScript d'Acrobat :-)
- sous Windows : créer un `pdflatex.exe` dans le répertoire courant

Conclusion

Au final, le langage LaTeX n'est pas trop dangereux dans sa configuration par défaut (sous debian du moins).

Recommandation : ne jamais compiler une source latex provenant de source non fiable.