

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Débordement de variable dans gv

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2002-AVI-227>

Gestion du document

Référence	CERTA-2002-AVI-227-002
Titre	Débordement de variable dans gv
Date de la première version	15 octobre 2002
Date de la dernière version	31 octobre 2002
Source(s)	CVE CAN-2002-0838 Alerte SUN : 47780 Avis de sécurité Debian DSA 176-1 Avis de sécurité Mandrake MDKSA-2002-069 et MDKSA-2002-071
Pièce(s) jointe(s)	Aucune

TAB. 1 – gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

Exécution de code arbitraire.

2 Systèmes affectés

- gv versions 3.5.8 et précédentes ;
- ggv versions 1.0.2 et précédentes ;
- KGhostView livré avec les versions 1.1 à 3.0.a du projet KDE.

dans des architectures de processeur i386 ou alpha.

3 Résumé

Une vulnérabilité dans les logiciels gv, ggv et KGhostView permet par le biais d'un document PostScript ou PDF astucieusement construit d'exécuter un code arbitraire.

4 Description

4.1 La vulnérabilité

`ghostscript` est un logiciel qui interprète les langages `PostScript` et `Portable Document Format (PDF)` et qui s'utilise en ligne de commande pour, le plus souvent :

- afficher un fichier `PostScript` ou `PDF` à l'écran ;
- imprimer un tel fichier sur une imprimante qui ne connaît pas le `PostScript` ;
- ainsi que diverses autres manipulations du `PostScript` ou du `PDF`.

`gv` est une interface graphique qui dispense d'utiliser `ghostscript` en ligne de commande. `gv` est utilisé pour lire à l'écran un fichier `PostScript` ou `PDF`.

`ggv` est l'intégration du logiciel `gv` dans le projet `GNOME`.

`KGhostView` est l'intégration du logiciel `gv` dans le projet `KDE`. Le logiciel `KGhostView` est contenu dans le paquetage `kdegraphics`.

Un débordement de variable dans le programme `gv` (versions 3.5.8 et inférieures) permet à un utilisateur mal intentionné de construire un fichier `PDF` ou `PostScript` et inciter un utilisateur naïf à le visualiser avec `gv`. Ce fichier astucieusement construit, lors de sa visualisation par le biais des versions vulnérables de `gv`, exécute un code choisi par l'utilisateur mal intentionné.

`ggv` étant un développement basé sur `gv`, les versions de `ggv` antérieures à 1.0.2 sont vulnérables à ce débordement de variables.

`KGhostView` est aussi basé sur `gv`. Les versions non corrigées antérieures à la version 3.0.4 de `kdegraphics` sont vulnérables.

4.2 Suis-je vulnérable ?

Pour déterminer la version de `gv`, il suffit d'entrer la commande suivante dans un terminal :

```
$ gv -v
gv 3.5.8
$
```

Ici la version de `gv` est vulnérable.

```
$ ggv --version
Gnome gnome-ghostview 1.1.96
$
```

Cette version de `ggv` n'est pas vulnérable.

```
$ kghostview -v
Qt: 2.3.1
KDE: 2.2.2
KGhostView 0.12
$
```

Cette version de `KGhostView` est vulnérable.

5 Solution

Si vous utilisez `ggv`, assurez-vous qu'il s'agit d'une version récente de `ggv` (version supérieure à 1.0.2), si besoin, mettre à jour `ggv`.

Si vous utilisez `KDE`, mettez à jour `KGhostView`. Des patches sont disponibles sur le site `ftp` du projet `KDE`, pour les versions 2.2.2 et 3.0.3 de `KDE`. Une autre solution est d'utiliser une version récente de `kdegraphics`. La version 3.0.4 corrige cette vulnérabilité.

Certains vendeurs proposent des correctifs pour cette vulnérabilité, par exemple :

Mandrake <http://www.mandrakesecure.net/en/advisories/2002/MDKSA-2002-069.php>
<http://www.mandrakesecure.net/en/advisories/2002/MDKSA-2002-071.php>

RedHat <https://rhn.redhat.com/errata/RHSA-2002-207.html>

SUN Linux http://sunsolve.Sun.COM/pub-cgi/retrieve.pl?doc=fsalert%2F47780&zone_32=category%3Asecurity

Debian <http://www.debian.org/security>

6 Documentation

- Le logiciel `gv` est fournit par le site
<http://wwwthep.physik.uni-mainz.de/plass/gv> ;
- Les logiciel `ggv` est développé dans le cadre du projet GNOME :
<ftp://ftp.gnome.org/pub/gnome/sources/ggv>
- Le projet KDE propose des correctifs sur le site
ftp://ftp.kde.org/pub/kde/security_patches
- la version de `KGhostView` à jour (vis-à-vis de cette vulnérabilité) est disponible à l'adresse suivante dans le paquetage `kdegraphics` :
<http://download.kde.org/stable/3.0.4>

Gestion détaillée du document

15 octobre 2002 version initiale.

18 octobre 2002 ajout de la référence SUN Linux et Debian.

31 octobre 2002 ajout de la référence Mandrake Linux.