

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Débordement de pile dans le programme splitVT

---

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-2000-AVI-010>

---

### Gestion du document

Référence	CERTA-2000-AVI-010
Titre	Débordement de pile dans le programme <code>splitVT</code>
Date de la première version	20 juin 2000
Date de la dernière version	–
Source(s)	Security Bugware avis debian du 5 juin 2000 BugTrack
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

- usurpation locale des privilèges du superutilisateur `root` sur la machine accueillant `splitVT` ;
- capture de mots de passe.

Le risque existe puisqu'un programme d'exploitation de la vulnérabilité a été publié.

## 2 Systèmes affectés

La version 1.6.3 de `splitVT` (utilitaire pour UNIX).

## 3 Résumé

`splitVT` est un programme qui découpe verticalement un terminal en deux parties ; chaque partie accueillant un shell différent. Un programme exploitant un débordement de variable dans la pile a été publié. Ce programme permet d'acquiescer les droits `root` localement.

## 4 Solution

### 4.1 Supprimer splitVT

L'auteur de splitVT reconnaît dans la page de manuel que son application n'est pas absolument sûre en mode SET-UID. Donc, si vous n'avez pas absolument besoin de ce programme, il faut le désinstaller.

### 4.2 Debian

debian organisation publiant une distribution du système Linux a publié un correctif rendant sûre l'utilisation de splitVT :

#### Source

- [http://security.debian.org/dists/stable/updates/source/splitvt\\_1.6.3-7.0slink1.diff.gz](http://security.debian.org/dists/stable/updates/source/splitvt_1.6.3-7.0slink1.diff.gz)
- [http://security.debian.org/dists/stable/updates/source/splitvt\\_1.6.3-7.0slink1.dsc](http://security.debian.org/dists/stable/updates/source/splitvt_1.6.3-7.0slink1.dsc)
- [http://security.debian.org/dists/stable/updates/source/splitvt\\_1.6.3.orig.tar.gz](http://security.debian.org/dists/stable/updates/source/splitvt_1.6.3.orig.tar.gz)

**alpha** [http://security.debian.org/dists/stable/updates/binary-alpha/splitvt\\_1.6.3-7.0slink1\\_alpha.deb](http://security.debian.org/dists/stable/updates/binary-alpha/splitvt_1.6.3-7.0slink1_alpha.deb)

**i386** [http://security.debian.org/dists/stable/updates/binary-i386/splitvt\\_1.6.3-7.0slink1\\_i386.deb](http://security.debian.org/dists/stable/updates/binary-i386/splitvt_1.6.3-7.0slink1_i386.deb)

**m68k** [http://security.debian.org/dists/stable/updates/binary-m68k/splitvt\\_1.6.3-7.0slink1\\_m68k.deb](http://security.debian.org/dists/stable/updates/binary-m68k/splitvt_1.6.3-7.0slink1_m68k.deb)

**sparc** [http://security.debian.org/dists/stable/updates/binary-sparc/splitvt\\_1.6.3-7.0slink1\\_sparc.deb](http://security.debian.org/dists/stable/updates/binary-sparc/splitvt_1.6.3-7.0slink1_sparc.deb)

### 4.3 Nouvelle version de splitVT

On peut mettre à jour son système en chargeant la dernière version de splitVT :

<http://www.devolution.com/slouken/projects/splitvt/splitvt-1.6.4.tar.gz> .

### 4.4 Suse

La version de splitVT installée dans la distribution Suse n'est pas sensible à cette vulnérabilité. Cependant, elle est installée dans une configuration qui pourrait permettre, entre autre, de capturer ce qui est entré au clavier (par exemple un mot de passe).

Il faut la remplacer par la version 1.6.4 décrite plus haut (compilée par vos soins).

## 5 Documentation

### Gestion détaillée du document

20 juin 2000 version initiale.