Projet SDTD - Pile SMACK

Analyse de la corrélation entre données météorologiques et tweets

Documentation

Pablo Cabrera Ludovic Carre Yann Colina
Maxime Deloche Guilaume Dubois Vincent Lefoulon
Nicolas Meyer Clément Parizot

3^{rd} – Specialization ISI

19 Janvier 2017

Contents

1 Compromission

Le service compromis est la bibliothèque standard C, GNU C Library (glibc). Cette librairie est utilisée par différents types de systèmes : différents types de noyaux et différents types d'architectures. Elle est surtout présente dans les systèmes Linux sur une architecture x86. La glibc est notamment présente sur CentOS, Ubuntu, RedHat, Suse, Ubuntu, Fedora...

Il s'agit d'une compromission de type Local Exploit et référencée comme stack clash.

2 Vulnérabilité

Merci de prendre connaissance de la faille CVE-2017-1000366 rencontrée dans nos systèmes et d'agir suivant les recommandations du département de sécurité informatique.

```
CVE-2017-1000366
├── Type
│   ├── Local exploit
│   └── Stack smashing
├── Service compromis
│   └── Bibliothèque standard C, GNU C Librairy (glibc)
├── Systèmes affectés
│   ├── Linux, architecture x86
│   └── OS : CentOS, Ubuntu, RedHat, Suse, Ubuntu, Fedora
└── Compromission
    ├── Confidentialité [Totalement compromis]
    ├── Intégrité [Totalement compromis]
    └── Authentifications [outrepassées]
```

3 Expérimentations

Bibliographie

- http://www.cvedetails.com/cve/CVE-2017-1000366/
- https://www.exploit-db.com/exploits/42275/
- https://www.suse.com/support/kb/doc/?id=7020973
- https://securitytracker.com/id/1038712
- https://www.qualys.com/2017/06/19/stack-clash/stack-clash.txt