Numéro

1

Bulletin de Sécurité

Juin 2011

Rédigé par Nabil OUCHN& Youssef MANAR

http://cert.netpeas.org

- Lancement du CERT-NETPEAS le 1er Juin 2011. Le cahier des charges ainsi que les délais ont été scrupuleusement respectés.

- Un Grand Message d'encouragement reçu de nos confrères du CERT SG France.

- Le CERT-NETPEAS est le premier organisme à avoir émis une alerte suite à la fuite d'information ciblant des mots de passe appartenant aux ministères marocains. Toutes les personnes incriminées ont été alertées.

- Travail collaborative avec un CERT Français pour la traque et la fermeture de plusieurs serveurs marocains utilisés pour une attaque de type Phishing contre une banque française (Banque Postale).

- Découverte et escalade vers les principaux CERT mondiaux (US-CERT, CERT, CERT Lexsi) d'une faille de sécurité logicielle d'un produit largement utilisé par les compagnies aériennes. Les CERT US-CERT et CERT Lexsi ont relayé notre « Alerte », en nous remerciant au passage, vers les compagnies américaines et françaises.

- Nous avons aussi subi plus de 11 329 attaques(and counting) tentant de paralyser nos activités. Les attaques étaient principalement émanant du Maroc. Les adresses IPont été bannies de nos infrastructures.

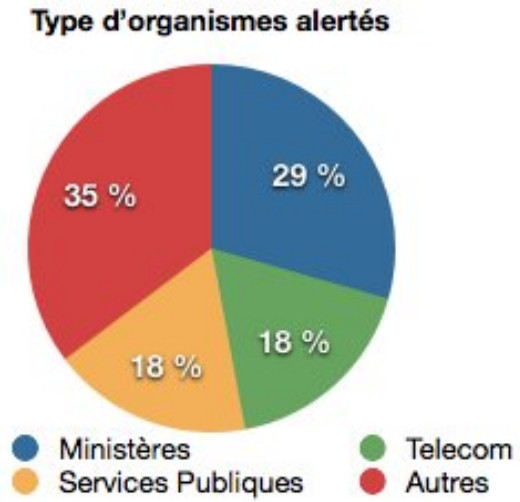
Statistiques (CERT-NETPEAS)

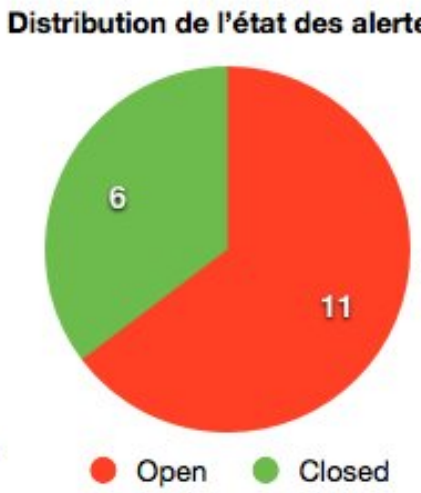
17 tickets incidents

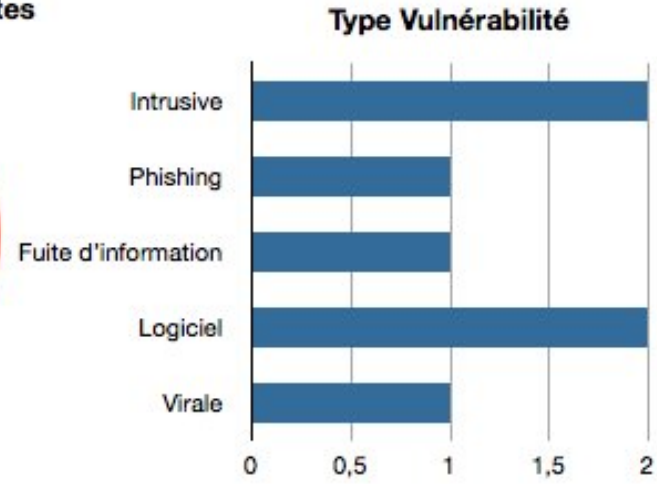
6 clos

7 Alertes

2 Critiques





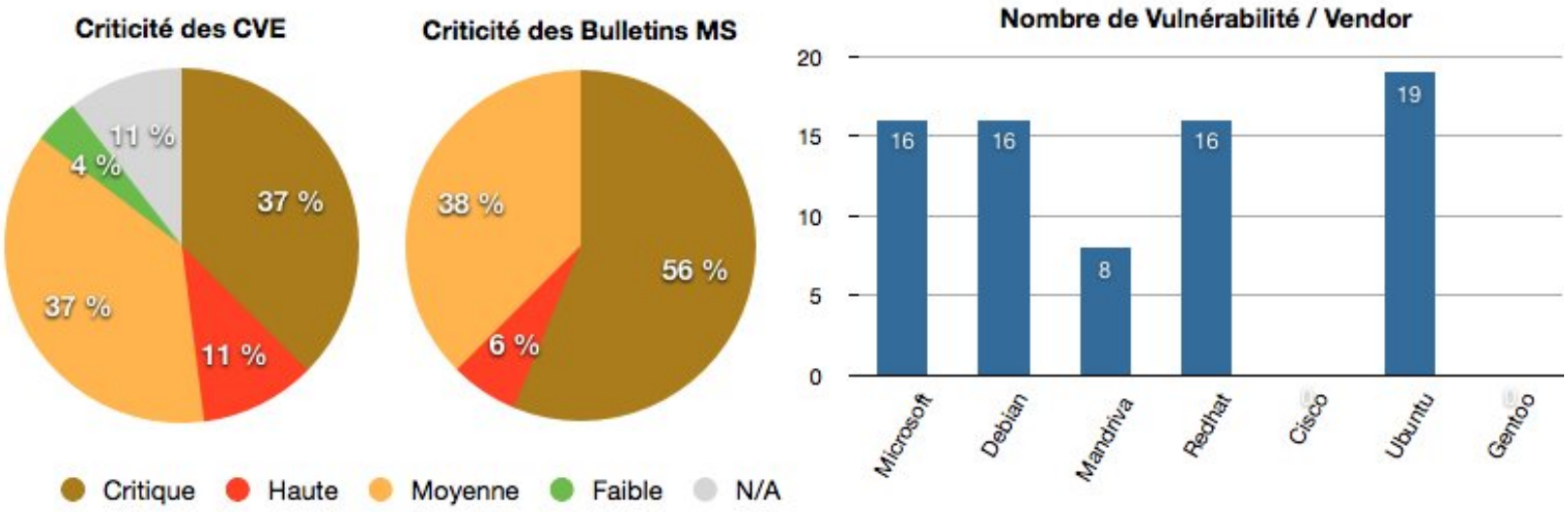


Source : cert.netpeas.org

Statistiques Vulnérabilités

246 CVE (Common Vulnerability Exposure)

16 Bulletins Microsoft



Source : VulnerabilityDatabase.com (notre site de veille vulnérabilité)
Risk Rating : Basé sur le système de scoring CVSS[1] v2.0 (Common Vulnerability Scoring System)
Critical : 9-10 | High 7-8.9 | Medium 4-6.9 | Low 0.1-3.9

[1] http://www.first.org/cvss

Top 10 des vulnérabilités les plus critiques

Les vulnérabilités les plus critiques sont calculées avec cette formule

Top Vulnérable = CVSS ((Base score) & (Impact score) & (Exploit score)) = 10

Fournisseur	Produit	CVE
Simplemachines	Smf 2.0	CVE-2011-1127
Adobe	Flash Player 9.125.0	CVE-2011-2110
Microsoft	Windows Xp	CVE-2011-1268
Microsoft	Windows Xp	CVE-2011-1868
Microsoft	Forefront Threat Management Gateway (TMG) 2010	CVE-2011-1889
Adobe	LiveCycle Data Services 3.1 and earlier, LiveCycle 9.0.0.2 and earlier, and BlazeDS 4.0.1	CVE-2011-2092
Sun	Jre 1.6.0	CVE-2011-0802 CVE-2011-0814 CVE-2011-0815 CVE-2011-0817