Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Affaire suivie par :
BeeRump

Paris, le 16 juin 2016
N° CVE-2015-6550

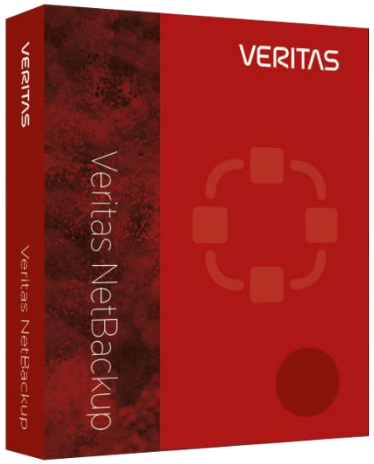
APT CYBER-NUMERIQUE SUR SAUVEGARDICIEL CONNECTE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Affaire suivie par :
BeeRump

Paris, le 16 juin 2016
N° CVE-2015-6550

APT CYBER-NUMERIQUE SUR SAUVEGARDICIEL CONNECTE



+

=

WTF is this ?

```
Host is up (0.89s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
1556/tcp  open  unknown
13701/tcp open  netbackup
13720/tcp open  netbackup
13721/tcp open  netbackup
13723/tcp open  unknown
13724/tcp open  unknown
```

(Veritas | Symantec) Netbackup

- Solution de sauvegarde multiplateforme (Windows, Linux, UNIX)
- Très fréquemment rencontrée lors de pentests
- Date de 1990, 5 rachats successifs

  ➔ Vulns. legacy ++

- 3 types de serveurs
  - Agents : serveurs backupés (filers, BDD, DC, …)
  - Media : stockage des backups
  - Master : gestion centralisée

Once upon a time…

Veritas » Netbackup : Security Vulnerabilities

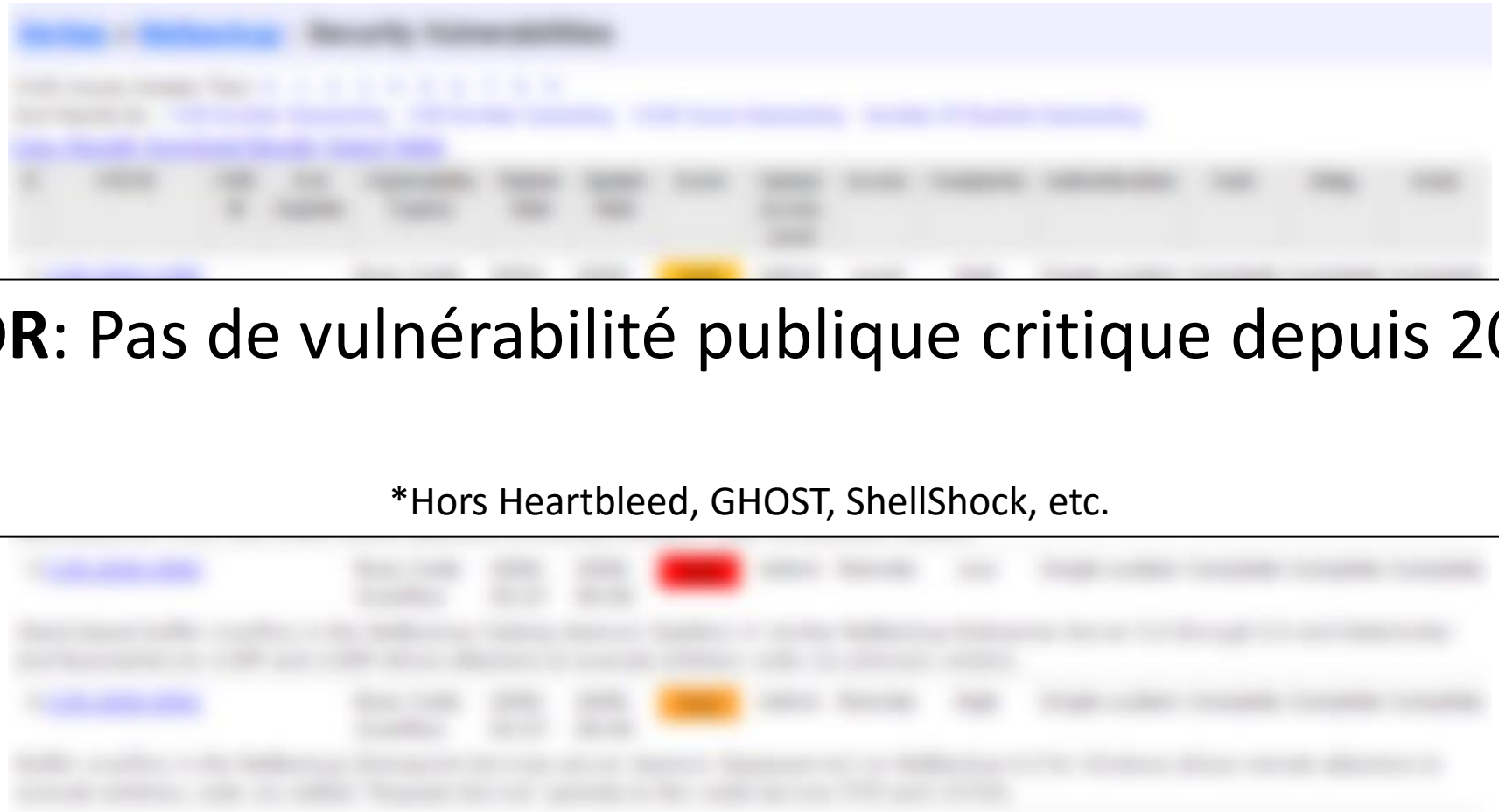
CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results Select Table

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2004-1389			Exec Code	2004-12-31	2008-09-05	6.0	Admin	Local	High	Single system	Complete	Complete	Complete
	Unknown vulnerability in the Veritas NetBackup Administrative Assistant interface for NetBackup BusinesServer 3.4, 3.4.1, and 4.5, DataCenter 3.4, 3.4.1, and 4.5, Enterprise Server 5.1, and NetBackup Server 5.0 and 5.1, allows attackers to execute arbitrary commands via the bpjava-susvc process, possibly related to the call-back feature.													
2	CVE-2006-0989			Exec Code Overflow	2006-03-27	2008-09-05	9.0	Admin	Remote	Low	Single system	Complete	Complete	Complete
	Stack-based buffer overflow in the volume manager daemon (vmd) in Veritas NetBackup Enterprise Server 5.0 through 6.0 and DataCenter and BusinesServer 4.5FP and 4.5MP allows attackers to execute arbitrary code via unknown vectors.													
3	CVE-2006-0990			Exec Code Overflow	2006-03-27	2008-09-05	9.0	Admin	Remote	Low	Single system	Complete	Complete	Complete
	Stack-based buffer overflow in the NetBackup Catalog daemon (bpdbm) in Veritas NetBackup Enterprise Server 5.0 through 6.0 and DataCenter and BusinesServer 4.5FP and 4.5MP allows attackers to execute arbitrary code via unknown vectors.													
4	CVE-2006-0991			Exec Code Overflow	2006-03-27	2008-09-05	7.1	Admin	Remote	High	Single system	Complete	Complete	Complete
	Buffer overflow in the NetBackup Sharepoint Services server daemon (bpspsserver) on NetBackup 6.0 for Windows allows remote attackers to execute arbitrary code via crafted "Request Service" packets to the vnetd service (TCP port 13724).													

Once upon a time…



TL;DR: Pas de vulnérabilité publique critique depuis 2006*

*Hors Heartbleed, GHOST, ShellShock, etc.


CHALLENGE
ACCEPTED
quickmeme.com

Ports en écoute

- Sur une installation par défaut (version 7.6.0.3) :

Port (TCP)	Service	Master	Media	Agent
1556	**veritax_pbx**	**ouvert**	**ouvert**	**ouvert**
13701	vmd	ouvert	ouvert	fermé
13720	bprd	ouvert	fermé	fermé
13721	bpdbm	ouvert	fermé	fermé
13723	bpjobd	ouvert	fermé	fermé
13724	vnetd	ouvert	ouvert	ouvert
13782	**bpcd**	**ouvert**	**ouvert**	**ouvert**
13783	nbatd	ouvert	fermé	fermé

(Ports écoutant en 0.0.0.0 uniquement)

Services

Nom	Description	État	Type de démarrage	Ouvrir une session en tant que
NetBackup Agent Request Server	Populates...	Démarré	Automatique	Système local
NetBackup Audit Manager	Manages ...	Démarré	Automatique	Système local
NetBackup Authentication	NetBacku...	Démarré	Automatique	Système local
NetBackup Authorization	NetBacku...		Désactivé	Système local
NetBackup Bare Metal Restore Master Server	Manages ...		Automatique	Système local
NetBackup Client Service	Client Ser...	Démarré	Automatique	Système local
NetBackup CloudStore Service Container	Provides c...	Démarré	Automatique	Système local
NetBackup Compatibility Service	This servi...	Démarré	Automatique	Système local
NetBackup Database Manager	Manages ...	Démarré	Automatique	Système local
NetBackup Deduplication Engine	Processes...		Désactivé	Système local
NetBackup Deduplication Manager	Manages ...		Désactivé	Système local
NetBackup Deduplication Multi-Threaded Agent	Provides ...	Démarré	Automatique	Système local
NetBackup Device Manager	Starts the...		Automatique	Système local
NetBackup Discovery Framework	Discovers ...	Démarré	Automatique	Système local
NetBackup Enterprise Media Manager	Keeps tra...	Démarré	Automatique	Système local
NetBackup Event Manager	Creates a...	Démarré	Automatique	Système local
NetBackup Indexing Manager	Manages ...	Démarré	Automatique	Système local
NetBackup Job Manager	Starts job...	Démarré	Automatique	Système local
NetBackup Key Management Service	The NetB...		Automatique	Système local
NetBackup Legacy Client Service	Listens fo...	Démarré	Automatique	Système local
NetBackup Legacy Network Service	Legacy N...	Démarré	Automatique	Système local
NetBackup Policy Execution Manager	Creates a...	Démarré	Automatique	Système local
NetBackup Proxy Service	Executes ...		Manuel	Système local
NetBackup Relational Database Manager	Manages ...	Démarré	Automatique	Système local
NetBackup Remote Manager and Monitor Service	Enables N...	Démarré	Automatique	Système local
NetBackup Request Daemon	Processes...	Démarré	Automatique	Système local
NetBackup Resource Broker	Allocates ...	Démarré	Automatique	Système local
NetBackup SAN Client Fibre Transport Service	Implemen...		Désactivé	Système local
NetBackup Service Layer	Gateway ...	Démarré	Automatique	Système local
NetBackup Service Monitor	Monitors t...	Démarré	Automatique	Système local
NetBackup Storage Lifecycle Manager	Manages ...	Démarré	Automatique	Système local
NetBackup Vault Manager	Manages ...	Démarré	Automatique	Système local
NetBackup Volume Manager	Acts as a ...	Démarré	Automatique	Système local
NetBackup Web Management Console	Serves re...		Désactivé	Système local

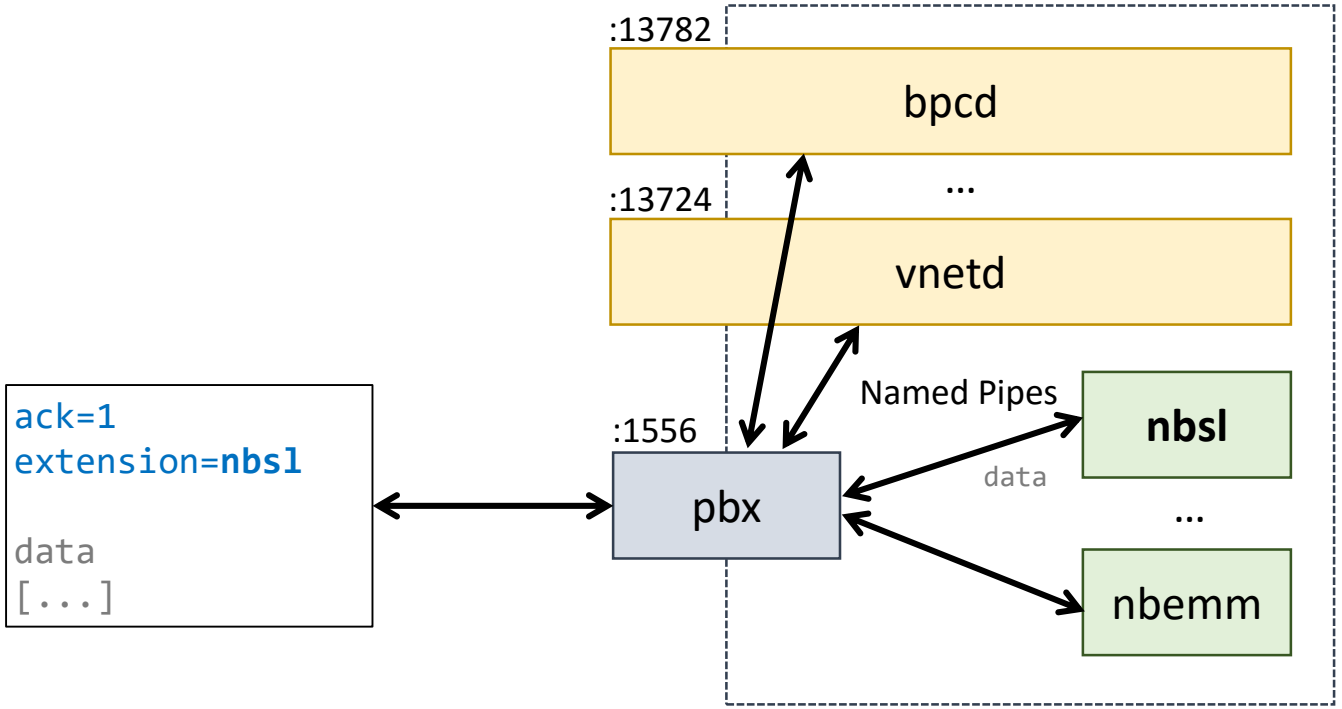
ou root (Linux/UNIX)

ou admin de domaine

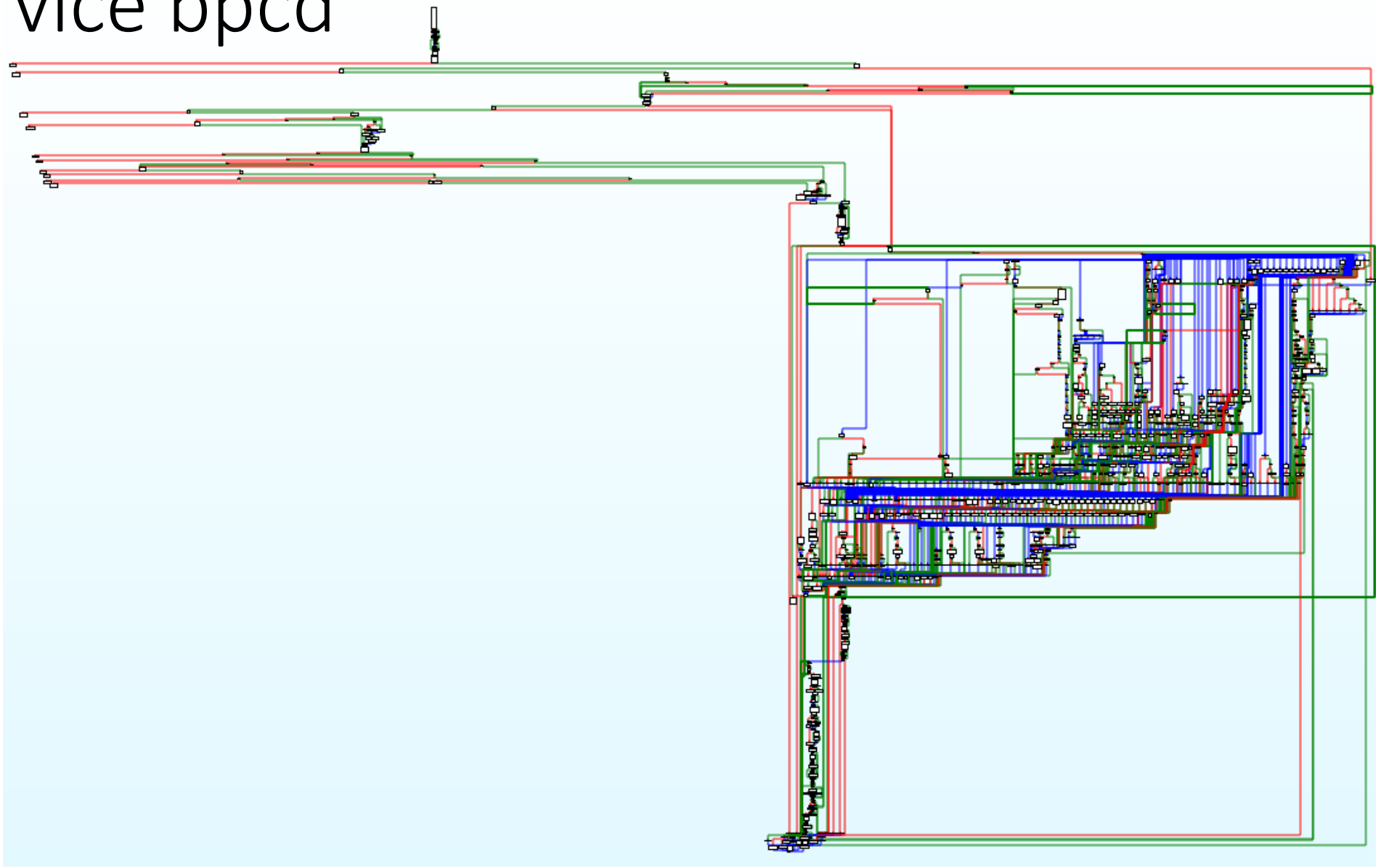
Service PBX

- Sorte de (reverse) proxy
  - Rend accessibles les services n'écoutant pas sur 0.0.0.0
- Va remplacer à terme les services legacy

➔ One port to bind them all!



Service bpcd



Service bpcd

- Tourne partout: agents, media et master servers
- Utilisé conjointement avec le service **vnetd**
- Protocole binaire maison
- Features
  - Récupération d'informations
  - Listing/lecture/écriture de fichiers
  - Exécution de commandes

Service bpcd : Authentification

- Basée sur le **hostname** du client
  - Résolution inverse via `getpeername()` et `getaddrinfo()`
    - Sous Windows : Requête NBNS de type NBSTAT
    - Sous Linux : Requête DNS de type PTR
  - Hostname comparé avec une liste blanche
    - Définie à l'installation (conf)
    - Limitée normalement au master et aux media servers

Service bpcd : Authentification

- Authentification : contournable
  - Interrogation de **vnetd** pour récupérer le nom du master
  - Target Windows : Responder NBSTAT
    - Prérequis : absence de filtrage entrant & sortant du port 137/udp
  - Target Linux : Spoofer de réponses DNS PTR
    - Prérequis: être en MITM entre la cible et son serveur DNS (même subnet)

- Exécution de commandes : filtrage, mais contournable
  - Windows : `"vltrun <cmd>"`
  - Linux : `"/usr/openv/netbackup/bin/../../../../../<cmd>"`

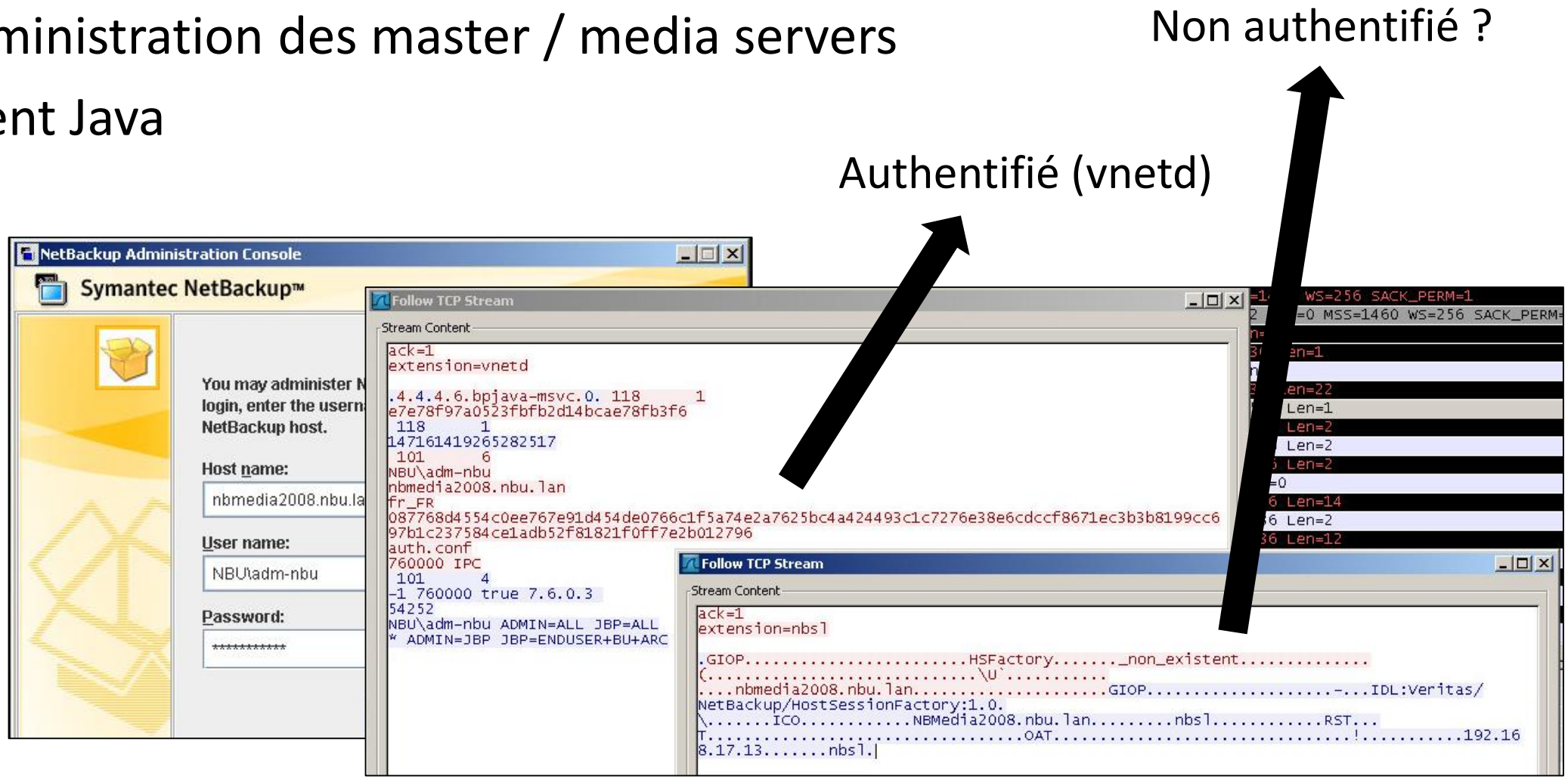
➔ CVE-2015-6550 : Remote root|SYSTEM

Service nbsl

- Administration des master / media servers
- Client Java

Service nbsl

- Administration des master / media servers
- Client Java



Service nbsl : RE de protocole

- Reconnu comme du « GIOP » par Wireshark
- GIOP = protocole **CORBA** permettant la communication entre « ORB »
- CORBA TL;DR:
  - Appel de méthodes à distance
  - Fichier .idl compilé en fichier source dans le langage cible (.java, .cpp)
  - Type mapping entre IDL et langage cible
  - Stubs dans le client et le serveur
- Ici, variante propriétaire : **PBXIOP**
- **Non authentifié par défaut**

Service nbsl : PBXIOP & IDL

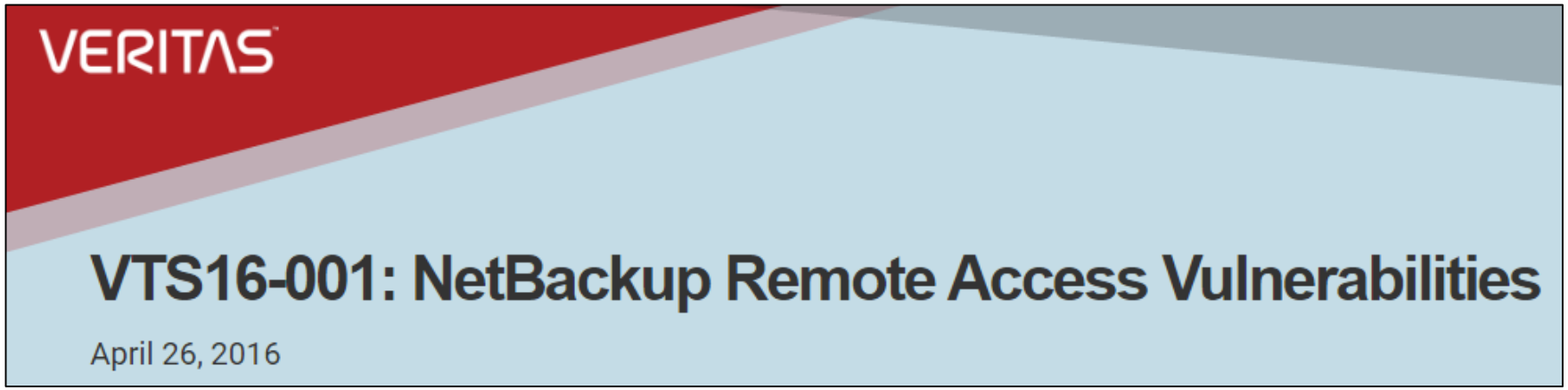
- Approches :
  - Reconstituer l'IDL et recoder un ORB compatible PBXIOP
  - **Instrumenter le code existant**
- RE très fastidieux
  - *nbsl.exe* : C++, 11 Mo, 72k fonctions
  - **servicelayer.jar** ➔ Androguard, Jython
- ~2 mois plus tard, on obtient :
  - Un IDL de 20k lignes
  - Un shell pour requêter en CORBA sans authentification ☺

Service nbsl : so what ?

- Accès à toutes les features des master/media servers sans authent.
  - Lancement de backup arbitraire
  - Restauration de backup arbitraire
  - Parcours des backups existantes

- Scénarios
  - Exfiltration de backups contenant des données sensibles
  - Compromission via backup d'un DC
  - Backdooring du fichier `~/.ssh/authorized_keys` d'une machine cible
    - Sauvegarde, modification et restauration

➔ CVE-2015-6552 : Bypass d'authentification sur console d'administration



Severity

	CVSS2 Base Score	Impact	Exploitability	CVSS2 Vector
CVE-2015-6550*	Communications Protocol Remote Command Execution			
	9.3	10	8.6	AV:N/AC:M/Au:N/C:C/I:C/A:C
CVE-2015-6551*	Weak Key Exchange Exposure			
	7.9	10	5.5	AV:A/AC:M/Au:N/C:C/I:C/A:C
CVE-2015-6552*	Management Services Allow Unauthorized RPC			
	9.3	10	8.6	AV:N/AC:M/Au:N/C:C/I:C/A:C

* L'auteur s'excuse pour l'absence de logo et de site Web dédiés à ces vulnérabilités

Conclusion

- Netbackup, une cible de choix
  - Surface d'attaque conséquente
  - Aucune défense en profondeur par défaut

- 3 vulnérabilités présentes par défaut sur toutes les installations <= 7.7.1
  - Liées à l'authentification (implémentation et design)
  - Certaines nécessitent plus de travail que d'autres
  - Reportées en sept. 2015, corrigées en mai 2016

- Fix : version **7.7.2**
  - Disclaimer : patch non testé, *feel free* ☺

Questions ?

Bonus

Services vnetd & bpjava-msvc : TL;DR

- Tourne sur agents, media et master servers
- Protocole maison, mélange d'ASCII et de binaire
- 2 types de commandes : avec et sans authentification
- Authentification basée sur un compte du système (local ou AD)
- Client en Java : console d'administration
- Algo crypto maison « VMangle »
  - Ciphertext = **XOR-CBC**(plaintext, MD5(rc + rs + CONST))
  - **Déchiffrable via capture passive**

➔ CVE-2015-6551

RE de PBXIOP – Reconstitution d'IDL

- Nbsl.exe : Parsing de RTTI
  - 1ere tentative avec IDAPython + ClassInformer
  - Les symboles sont présents sur certains binaires Linux
  - Au final, pas concluant
    - Certaines informations IDL sont perdues lors de la traduction en C++ puis compilation
- Utilisation d'***Androguard*** pour browser servicelayer.jar
  - Effectuer la traduction inverse : Java => IDL
  - Nécessite quelques ajustements manuels (java.lang.String => C String ou Unicode?)
  - Accès uniquement aux classes dont le stub est présent dans le client
- Certaines méthodes CORBA ne sont pas implémentées côté serveur ☺
  - Exception CORBA NO_IMPLEMENT

RE de PBXIOP – Instrumentation

- Tentative avec **JavaSnoop**, mais trop lourd
- Script ***Jython*** important *servicelayer.jar*
  - Connexion CORBA à l'objet `nbsl/HSFactory`
  - Récupération de références sur d'autres objets de proche en proche
- Nécessite certains tricks pour que tout fonctionne
  - Surcharge du ClassLoader par défaut pour `Class.forName()`
  - Utilisation de la réflexion pour déprotéger les membres private/protected
  - Génération dynamique de classes « ValueType Factories »
  - …
- **Frida** anyone ?

Recommendations alternatives

- NBAC / VxSS
  - Wrapping des services *bpcd* & co dans SSL avec certificats clients
- Filtrage des flux entre agents et master/media servers
  - Risque d'être compliqué à terme avec PBX
- Ne pas installer d'agent sur un DC
  - Inutile car déjà répliqué par les mécanismes AD