Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 09 mai 2017
N° CERTFR-2017-ACT-019

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2017-ACT-019

1 - Désactivation du protocole SMBv1

Contexte

En avril 2017, des attaquants se faisant appeler les `Shadow Brokers` ont publiquement révélé des outils offensifs, qui proviendraient du groupe Equation, annoncé comme lié à la NSA. Quatre de ces outils permettent d'exploiter des vulnérabilités liées à SMBv1 (ETERNALROMANCE, ERRATICGOPHER, ETERNALCHAMPION et ETERNALBLUE). Le bulletin d'actualité `CERTFR-2016-ACT-039` du 26 septembre 2016 précise les faiblesses de ce protocole et rappelle que les systèmes d'exploitation supportant uniquement SMBv1 sont désormais obsolètes (Windows 2000, Windows XP et Windows 2003). Pour des raisons de compatibilité, Microsoft continue d'activer ce protocole, même dans les versions récentes de Windows. Il est ainsi recommandé de désactiver SMBv1.

Audit du service

Avant de le désactiver, il est recommandé d'activer l'audit de l'utilisation de SMBv1. Comme le rappelle le bulletin d'actualité `CERTFR-2016-ACT-039`, la *cmdlet* PowerShell (Disponible à partir de Windows 2012 R2) :

```
Set-SmbServerConfiguration -AuditSmb1Access \$true
```

permet d'auditer l'utilisation de SMBv1 sur le système avant d'effectuer cette transition protocolaire.

Les journaux relatifs à l'audit de SMBv1 sont consultables grâce à l'observateur d'événements Windows (`Journaux Windows\Journaux des applications et des services\Microsoft\Windows\SMBServer\A`
La *cmdlet* PowerShell

```
Get-WinEvent -LogName Microsoft-Windows-SMBServer/Audit
```

Permet également de visualiser ces journaux.

Désactivation

Il est possible de désactiver SMBv1 sur tous les systèmes Windows. Ceci peut être effectué en désactivant le service de SMBv1 (`mrxsmb10`). Ceci nécessite cependant préalablement de retirer la dépendance liée à SMBv1 pour le service `lanmanworkstation`.

L'utilitaire `sc.exe` intégré à Windows permet d'effectuer cette manipulation :

```
sc.exe config lanmanworkstation depend = bowser/mrxsmb20/nsi
sc.exe config mrxsmb10 start = disabled
```

En plus de la désactivation, il est possible d'inhiber les fonctionnalités du client SMBv1 en positionnant la valeur 0 dans l'attribut SMB1 sous la clé de registre HKEY_LOCAL_MACHINE\ SYSTEM\CurrentControlSet \Services\LanmanServer\Parameters. (Cet attribut a été introduit à partir de Windows 8 et de Windows Server 2012.)

À partir de la version 3.0 de PowerShell intégrée à Windows 8 et à Windows Server 2012, la *cmdlet* PowerShell
`Disable-WindowsOptionalFeature -FeatureName SMB1Protocol -Online`
effectue cette manipulation.

Enfin, à partir de Windows 8.1 et Windows Server 2012 R2, SMBv1 peut être désinstallé grâce au gestionaire de fonctionnalités Windows. La *cmdlet* PowerShell suivante permet également d'effectuer cette manipulation :
`Disable-WindowsOptionalFeature -FeatureName SMB1Protocol -Online`

Le script PowerShell ci-dessous permet de désactiver SMBv1 sur n'importe quelle machine à partir de Windows 7. Celui-ci peut notamment être déployé et exécuté à l'aide des GPO dans le cadre d'un domaine Active Directory.

```
if ([Environment]::OSVersion.Version -ge (new-object 'Version' 10,0))
{
  Disable-WindowsOptionalFeature -FeatureName SMB1Protocol -Online
}
else
{
  Set-Service mrxsmb10 -StartupType Disabled
  $svc = Get-WmiObject win32_Service -filter "Name='LanmanWorkstation'"
  $svc.Change($null,$null,$null,$null,$null,$null,$null,$null,$null,
              $null,@('Bowser','MRxSmb20','NSI'))

  $RegKey = 'HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters'
  if ((Test-Path -Path $RegKey) -and
     (((Get-ItemProperty -LiteralPath $RegKey).psbase.members |
        %{$_.name}) -contains 'SMB1'))
  {
    Set-ItemProperty -Path $RegKey -Name SMB1 -Value 0
  }
}
```

2 - Rappel des avis émis

Dans la période du 01 au 07 mai 2017, le CERT-FR a émis les publications suivantes :

- CERTFR-2017-AVI-134 : Multiples vulnérabilités dans Mozilla Thunderbird
- CERTFR-2017-AVI-135 : Multiples vulnérabilités dans Google Android (Nexus)
- CERTFR-2017-AVI-136 : Vulnérabilité dans les micrologiciels Intel
- CERTFR-2017-AVI-137 : Multiples vulnérabilités dans Citrix XenServer
- CERTFR-2017-AVI-138 : Multiples vulnérabilités dans Google Chrome
- CERTFR-2017-AVI-139 : Multiples vulnérabilités dans les produits Cisco

Gestion détaillée du document

09 mai 2017 version initiale.