SECURITE WINDOWS

# Ouverture de session invité non sécurisée

Description de la faille

Les ouvertures de session invité non sécurisée sont utilisées par les serveurs de fichier pour autoriser l’accès non-authentifié aux dossiers partagés.  
Les ouvertures de session invité non sécurisées n’ayant pas recours à l’authentification, d’importantes fonctionnalités de sécurité comme la signature SMB ou le chiffrement SMB sont désactivé.   
  
Par conséquent, les clients qui autorisent les ouvertures de session invité non sécurisées sont vulnérables à tout un ensemble d’attaques Man in the Middle pouvant entrainer des pertes ou corruptions de données, et exposer à des malwares.   
En outre, toutes les données écrites sur un serveur de fichier en utilisant une ouverture de session invité non sécurisées sont potentiellement accessibles par n’importe quel membre du réseau.

Action du correctif de la faille  
  
Cette stratégie détermine si le client SMB autorisera les ouvertures de session invité non sécurisées à un serveur SMB.  
Si vous activez ou ne configurez pas cette stratégie, le client SMB autorisera les ouvertures de session invité non sécurisées.

Application corrective

Как нажать Win + R « *gpedit.msc »*  
  
**Stratégie Ordinateur local > Configuration ordinateur > Modèle d’administration > Réseau > Station de travail LANMAN  
« Activer les ouvertures de session invité non sécurisées »  
Désactiver.**

# Délégation d’informations d’identification

Description de la faille

Lorsque la délégation d'informations d'identification est utilisée, les appareils fournissent une version exportable des informations d'identification à l'hôte distant.  
Les utilisateurs courent alors le risque de voir leurs informations d'identification volées par des personnes malveillantes sur l'hôte distant.

Action du correctif de la faille  
  
Si vous activez ce paramètre de stratégie, l'hôte prend en charge le mode d'administration restreinte ou Credential Guard à distance.  
Si vous désactivez ou ne configurez pas Ce paramètre de stratégie, l’administration restreinte et le mode Guard pour les informations d’identification à distance ne sont pas pris en charge. L'utilisateur devra toujours transmettre ses informations d'identification à l'hôte.

Application corrective

Как нажать Win + R « *gpedit.msc »*

**Stratégie Ordinateur local > Configuration ordinateur > Modèle d’administration > Système > Délégation d’informations d’identification**

**« L’hôte distant autorise la délégation d’informations d’identification non exportables »  
Activer.**

# Pilote de démarrage

Description de la faille  
  
Ce paramètre de stratégie vous permet de spécifier les pilotes de démarrage qui sont initialisés en fonction d’une classification déterminée par un pilote de démarrage de logiciel anti-programme malveillant à lancement anticipé.  
Le pilote de démarrage du logiciel anti-programme malveillant à lancement anticipé peut renvoyer les classifications suivantes pour chaque pilote de démarrage :  
-**Bon :** le pilote a été signé et n’a pas été falsifié.  
- **Mauvais :** le pilote a été identifié comme un programme malveillant. Nous vous recommandons de ne pas autoriser l’initialisation de mauvais pilotes.  
- **Mauvais, mais requis pour le démarrage :** le pilote a été identifié comme un programme malveillant, mais l’ordinateur ne peut pas démarrer correctement sans charger ce pilote.  
- **Inconnu :** Ce pilote a été attesté par votre application de détection de programme malveillant et n’a pas été classé par le pilote de démarrage de logiciel anti-programme malveillant à lancement anticipé.

Action du correctif de la faille

* Si vous activez ce paramètre de stratégie, vous pouvez choisir quels pilotes de démarrage initialiser au prochain démarrage de l’ordinateur.
* Si vous désactivez ce paramètre de stratégie ou ne le configurez pas, les pilotes de démarrage classés dans les catégories Bon, Inconnu ou Mauvais mais critique pour le démarrage sont initialisés et les pilotes classés dans la catégorie Mauvais ne sont pas initialisés.
* Si votre application de détection de programme malveillant n’inclut pas de pilote de démarrage de logiciel anti-programme malveillant à lancement anticipé ou si ce pilote a été désactivé, ce paramètre n’a aucun effet et tous les pilotes de démarrage sont initialisés.

Application corrective  
  
Как нажать Win + R « *gpedit.msc »*

**Stratégie Ordinateur local > Configuration ordinateur > Modèle d’administration > Système > Logiciel anti-programme malveillant à lancement anticipé  
Activer.  
Bons, inconnus et mauvais mais critique.**

# Authentification Digest pour le client WinRM

Description de la faille  
  
Ce paramètre de stratégie permet de définir si le client Gestion à distance de Windows (WinRM) utilise l’authentification de Digest.

Action du correctif de la faille  
  
Si vous activez ce paramètre de stratégie, le client WinRM n’utilise pas l’authentification Digest.

Application corrective

Как нажать Win + R « *gpedit.msc »*

**Stratégie Ordinateur local > Configuration ordinateur > Composants Windows > Gestion à distance de Windows (WinRM) > Client WinRM**

**« Ne pas autoriser l’authentification Digest »  
Activer.**

# Informations d’identification RunAs du service WinRM

Description de la faille  
  
Ce paramètre de stratégie permet de définir si le service Gestion à distance de Windows (WinRM) n’accepte pas le stockage d’informations d’identification RunAs pour aucun plug-in.

Action du correctif de la faille

* Si vous activez ce paramètre de stratégie, le service WinRM n’autorise pas la définition des valeurs de configuration RunAsUser ou RunAsPassword pour aucun plug-in.
* Si un plug-in a déjà défini des valeurs de configuration RunAsUser et RunAsPassword, la valeur de configuration RunAsPassword est effacée de la banque d’informations d’identification sur l’ordinateur.

Application corrective  
  
Как нажать Win + R « *gpedit.msc »*

**Stratégie Ordinateur local > Configuration ordinateur > Composants Windows > Gestion à distance de Windows (WinRM) > Service WinRM**

**« Ne pas autoriser WinRM à stock des informations d’identification RunAs »  
Activer.**

# Configurer le client SMB v1

Description de la faille

* 1. Méthode Powershell

« *Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol* »

* 1. Méthode manuelle
     1. Panneau de configuration, Programmes et fonctionnalités
     2. Activer ou désactiver les fonctionnalités Windows
     3. Prise en charge du partage de fichiers SMB 1.0/CFIS (désactiver)
     4. Redémarrer l’ordinateur.

1. Délégation d’informations d’identification