

CCN-CERT BP/17



Recommandations de sécurité de Mozilla Firefox

RAPPORT DE BONNES PRATIQUES

MAI 2021

ccn-cert
centro criptológico nacional

CCN
centro criptológico nacional

Edit:



© Centre national de cryptologie, 2020

Date de sortie : mai 2020

LIMITATION DE LA RESPONSABILITÉ

Ce document est fourni conformément aux termes contenus dans le présent document, rejetant expressément toute garantie implicite qui pourrait y être liée. En aucun cas, le Centre National de Cryptologie ne peut être tenu responsable des dommages directs, indirects, fortuits ou extraordinaires dérivés de l'utilisation des informations et du logiciel indiqués, même s'il a été averti de cette possibilité.

AVIS JURIDIQUE

Il est strictement interdit, sans l'autorisation écrite du Centre National de Cryptologie, sous les sanctions prévues par la loi, de reproduire partiellement ou totalement ce document par quelque moyen ou procédé que ce soit, y compris la reprographie et le traitement informatique, et de distribuer des copies de celui-ci par location ou prêt public.

Index

1. À propos du CCN-CERT, certificat Gouvernemental National	4
2. Introduction	5
3. Object	6
4. Scope	6
5. Téléchargement, installation et configuration de Mozilla Firefox	7
5.1. Versions	8
5.2. Exigences minimales	11
5.3. Emplacement de l'installation	12
5.4. Téléchargement et installation de Mozilla Firefox	13
5.5. Appliquer les paramètres de sécurité et de confidentialité	17
5.6. Les valeurs des directives	19
6. Liste de contrôle (évaluation)	49
7. Décalogue de recommandations	51
ANNEXE A. Fichiers de paramètres de sécurité	53

1. À propos du CCN-CERT, certificat Gouvernemental National

Le CCN-CERT est la capacité de réponse aux incidents de sécurité informatique du Centre national de cryptologie, CCN, rattaché au Centre national de renseignement, CNI. Ce service a été créé en 2006 en tant que **CERT Gouvernemental National espagnol** et ses fonctions sont incluses dans la loi 11/2002 réglementant le CNI, le RD 421/2004 réglementant le CCN et dans le RD 3/2010, du 8 janvier, réglementant le schéma de sécurité nationale (ENS), modifié par le RD 951/2015 du 23 octobre.

Sa mission est donc de contribuer à l'amélioration de la cybersécurité espagnole, en étant le centre national d'alerte et de réponse qui coopère et aide à répondre rapidement et efficacement aux cyberattaques et à faire face activement aux cybermenaces, y compris la coordination au niveau public de l'État des différentes capacités de réponse aux incidents ou des centres opérationnels de cybersécurité existants.

F de la loi 11/2002) et des informations sensibles, défendre le patrimoine technologique de l'Espagne, former du personnel spécialisé, appliquer des politiques et des procédures de sécurité et utiliser et développer les technologies les plus appropriées à cette fin.

Conformément à ce règlement et à la loi 40/2015 sur le régime juridique du secteur public, le CCN-CERT est chargé de la gestion des cyberincidents affectant tout organisme ou entreprise publique. Dans le cas des opérateurs critiques du secteur public, la gestion des cyberincidents sera assurée par le CCN-CERT en coordination avec le CNPIC.

Le CCN-CERT est la Capacité de Réponse aux Incidents de Sécurité de l'Information du Centre National de Cryptologie.

2. Introduction

Ce document fait partie de la documentation émise par le Centre National de Cryptologie dont l'objectif est de préserver la sécurité des systèmes TIC des Administrations Publiques.

À cette fin, un fichier de configuration est fourni pour appliquer des mesures de sécurité sur un *logiciel* de navigation sur Internet et faciliter ainsi la possibilité de mettre en œuvre la sécurité dans les systèmes TIC.

Pour l'élaboration de ce guide, nous avons utilisé le programme d'installation de *Mozilla Firefox* dans sa version 72.0.1 (64bit) pour Windows OS.

Pour l'élaboration de ce guide, nous avons utilisé le programme d'installation de Mozilla Firefox dans sa version 72.0.1 (64bit) pour Windows OS.

3. Objet

L'objectif de ce document est de présenter les procédures et les utilitaires nécessaires pour mettre en œuvre et assurer la sécurité dans *Mozilla Firefox*.



4. Scope

Ce document présente une procédure visant à améliorer la sécurité et à protéger *Mozilla Firefox* afin d'atténuer les vulnérabilités et les risques potentiels auxquels il peut être exposé.

Les utilisateurs de ce guide peuvent renforcer la sécurité de cette application grâce aux fichiers de configuration inclus dans son annexe.



5. Téléchargement, installation et configuration de Mozilla Firefox

Le programme Mozilla Firefox peut être téléchargé gratuitement sur le site web de Mozilla.

Mozilla Firefox doit avoir installé les dernières mises à jour logicielles liées à la sécurité. Pour ce faire, déterminez la méthode de mise à jour (par exemple, connexion à un serveur WSUS, procédure locale, mise à jour automatique, etc.)

Si les dernières mises à jour logicielles liées à la sécurité de Firefox ne sont pas appliquées, il s'agit d'une faille de sécurité critique.



Téléchargez le navigateur à l'adresse suivante : <https://www.mozilla.org/fr/firefox/new/>

5.1 Versions

Le logiciel de bureau Mozilla Firefox est disponible pour un déploiement avec les versions “fast” et “ESR”.

Rapid Release: recevez des mises à jour majeures toutes les six semaines et des mises à jour mineures, telles que des corrections de bogues et des correctifs de sécurité, selon les besoins pendant ces six semaines.

Extended Support Release (ESR) : en moyenne, vous recevez des mises à jour majeures toutes les 42 semaines et des mises à jour mineures, telles que des corrections de bogues, des corrections de sécurité et des mises à jour de politiques, selon les besoins, mais au moins toutes les six semaines.

En plus des différents cycles de mise à niveau, l'ESR a actuellement accès à des politiques supplémentaires qui ne sont pas disponibles dans la version rapide.






5.1 Versions

- Authentification intégrée (SPNEGO et NTLM).
- Désactiver les mises à jour des applications.
- Désactiver les mises à jour des modules complémentaires du système.
- Gérer les extensions.
- Changez la page d'accueil.
- Modifier la page Firstrun.
- Changez la page de mise à jour.
- Afficher la barre de recherche.
- Changement de moteurs de recherche.
- Filtrage des sites Web.

5.1 Versions

Pour savoir quelle version de Firefox vous utilisez:

Étapes	Description
1.	Cliquez sur le  bouton de menu, cliquez sur "Aide" et sélectionnez "À propos de Firefox". La fenêtre "À propos de Firefox" apparaît alors. Le numéro de la version installée s'affiche sous le nom de Firefox, comme le montre l'image suivante :
2.	
3.	Sinon, pour savoir quelle version du navigateur est installée, vous pouvez cliquer sur le  bouton de menu, puis sur "Aide" et sélectionner "Informations de dépannage". Cela ouvrira une page avec l'adresse "about:support" dans un nouvel onglet. La version de Firefox est indiquée dans la section Paramètres de base de l'application .

5.2 Exigences minimales

Voici la configuration minimale requise pour mettre en œuvre Mozilla Firefox sous Windows.

●	Système d'exploitation (32 bits et 64 bits)
○	Windows 7
○	Windows 8
○	Windows 10
●	Matériel recommandé
○	Processeur Pentium 4 ou plus récent prenant en charge SSE2.
○	512MB RAM / 2GB RAM pour la version 64-bit.
○	200 Mo d'espace disponible sur le disque dur.

5.3 Emplacement de l'installation

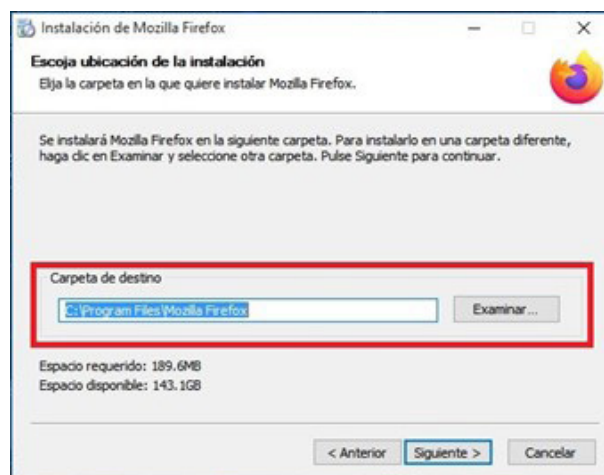
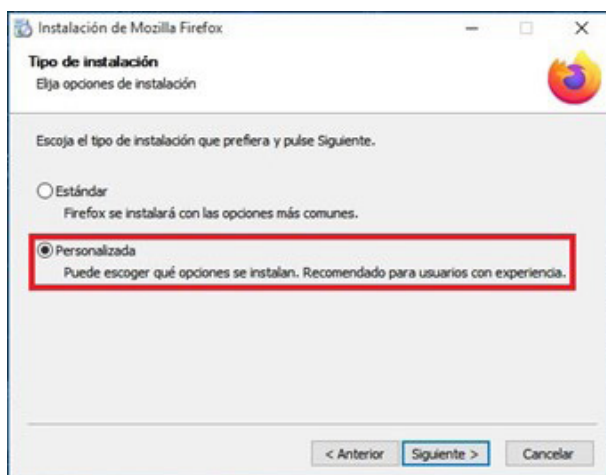
Les chemins d'installation de Mozilla Firefox sur un système d'exploitation Windows sont décrits ci-dessous :



C:\Program Files "Mozilla Firefox" est le chemin d'installation par défaut à la fois pour la version 32 bits (installée sur un système d'exploitation 32 bits) et la version 64 bits (installée sur un système d'exploitation 64 bits).



C:\Program Files(x86)\Mozilla Firefox est le chemin d'installation par défaut lors de l'installation du navigateur 32 bits sur un système d'exploitation 64 bits.




Remarque : Il est possible de personnaliser le chemin d'accès où le programme est installé pendant le processus d'installation.

5.4. Télécharger et installer Mozilla Firefox

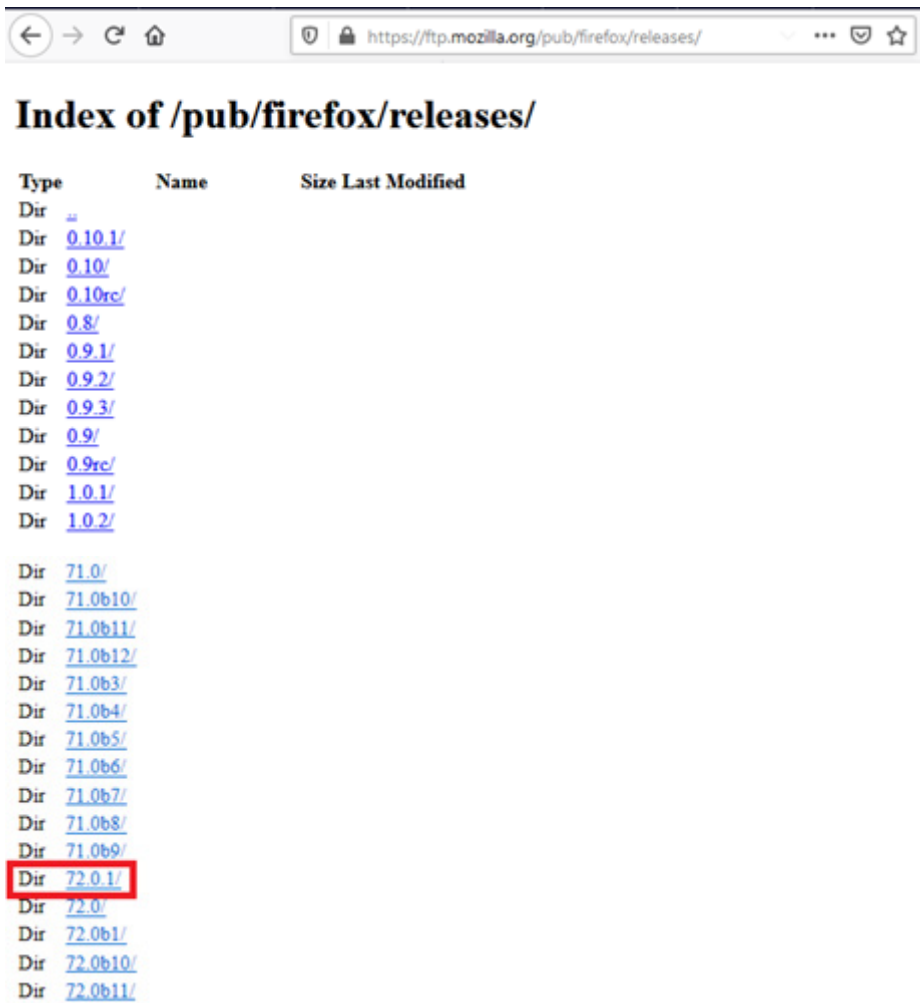
Il est possible de télécharger le programme par l'intermédiaire de l'url suivante:



<https://www.mozilla.org/es-ES/firefox/all/#product-desktop-release>

Étapes	Description
1.	<p>Dans cette fenêtre, sélectionnez le navigateur à télécharger, le système d'exploitation sur lequel ce téléchargement sera installé et enfin sélectionnez la langue. Cliquez ensuite sur le bouton "Télécharger maintenant" pour lancer le téléchargement du programme.</p> <p>Ce serait un exemple pour un téléchargement du navigateur Firefox en espagnol pour Windows 64 bits dans sa version la plus récente.</p>  <p>Remarque: Firefox Enterprise propose des installateurs MSI pour aider les administrateurs système à personnaliser et à déployer Firefox dans leurs environnements par le biais d'outils de déploiement Windows standard, tels que l'application de GPO dans Active Directory ou par le biais de Microsoft System Center Configuration Manager.</p> <p>https://support.mozilla.org/es/kb/personalizacion-de-firefox-con-instaladores-msi#w_msi-installers</p> <p>Une autre méthode alternative pour télécharger le navigateur est le FTP, à l'adresse suivante : https://ftp.mozilla.org/pub/firefox/releases/.</p>

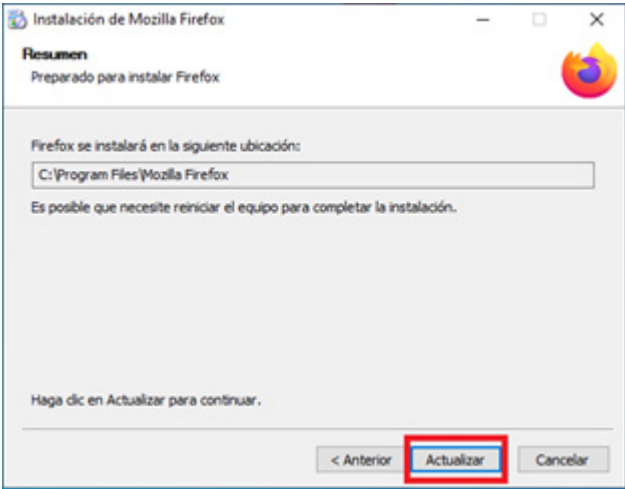
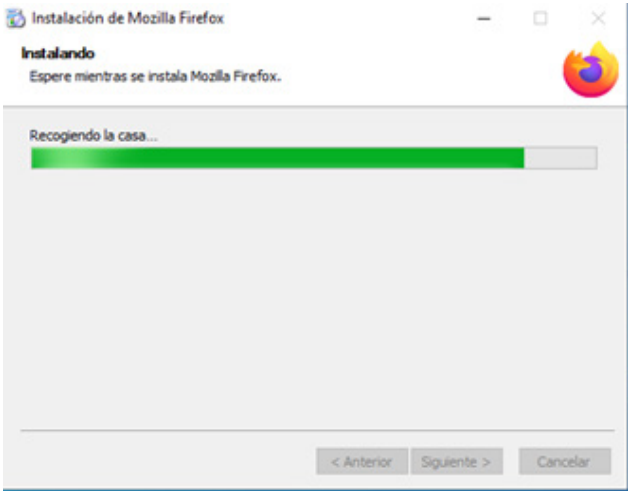
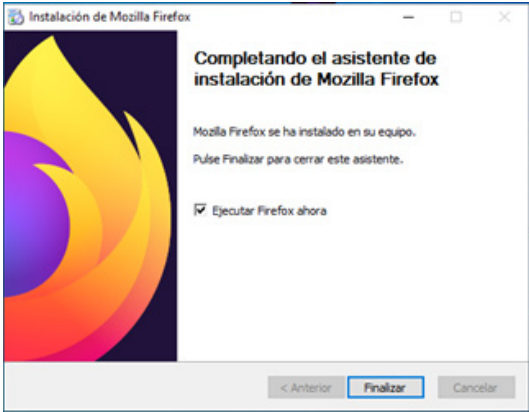
5.4. Télécharger et installer Mozilla Firefox

Étapes	Description
2.	<p>La fenêtre suivante servira d'exemple pour le téléchargement de Mozilla Firefox dans sa version 72.0.1.</p>  <p>Le fichier d'installation obtenu lors du téléchargement sera utilisé pour installer ou mettre à jour la version de Mozilla Firefox sur le système où les paramètres de sécurité et de confidentialité sont effectués.</p> <p>Pour lancer l'installation du navigateur, double-cliquez sur le fichier téléchargé.</p> <p>Note : Pour installer le programme, il est nécessaire de le faire avec un utilisateur ayant des privilèges d'administration sur l'ordinateur où vous installez Firefox.</p>

5.4. Télécharger et installer Mozilla Firefox

Étapes	Description
3.	<div></div> <p>Ensuite, procédez à l'installation du navigateur comme indiqué dans l'image ci-dessus.</p>
	<p>Mozilla Firefox installe par défaut un service facultatif appelé “service de maintenance”, qui permet d’effectuer des mises à jour en arrière-plan, sans que vous ayez à cliquer sur OK dans la boîte de dialogue Contrôle des comptes d’utilisateurs de Windows. Cette option peut être décochée lors de l’installation personnalisée.</p> <div></div> <p>Si une réinstallation de Firefox est effectuée sur une version existante, un bouton “Update” (mise à jour) apparaîtra à la place du bouton “Install” (installation), comme le montre l'image suivante:</p>

5.4. Télécharger et installer Mozilla Firefox

Étapes	Description
3.	
	<p>Une fois les étapes précédentes terminées, cliquez sur le bouton d'installation ou de mise à jour et attendez que le processus soit terminé.</p>
	 

ΔΔUne fois l'installation terminée, le système est redémarré et le navigateur peut être utilisé.

5.5. Appliquer les paramètres de sécurité et de confidentialité

Voici comment ajouter des paramètres de sécurité à Firefox pour assurer la sécurité de nos informations.

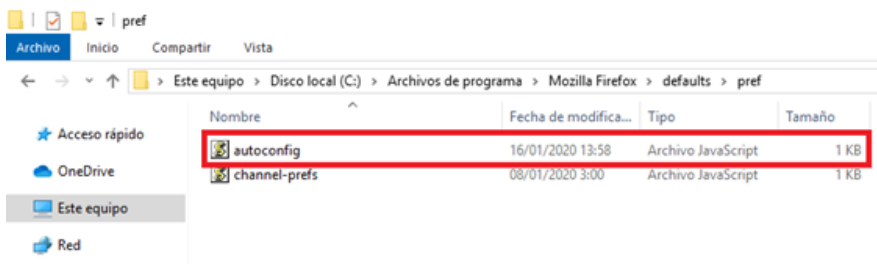
Les fichiers de configuration automatique peuvent être utilisés pour définir et verrouiller les préférences qui ne sont pas couvertes par les politiques de Firefox.

Pour utiliser la configuration automatique, deux fichiers doivent être placés dans les répertoires de Firefox.

Si le système d'exploitation est **Microsoft Windows**, ces fichiers seront situés dans le répertoire d'installation de Firefox.

Le fichier "**autoconfig.js**" est situé dans le répertoire "/Mozilla Firefox /defaults/pref".

Le fichier "**firefox.cfg**" est situé dans le répertoire d'installation de firefox ("/Mozilla Firefox").

Étapes	Description												
1.	<p>Le chemin d'installation par défaut est utilisé pour une installation de Mozilla Firefox en 64 bits:</p> <p>Le fichier “autoconfig.js” se trouve dans le répertoire C:\Program Files\Mozilla Firefox\defaults\pref.</p>  <table><tr><th>Nombre</th><th>Fecha de modifica...</th><th>Tipo</th><th>Tamaño</th></tr><tr><td>autoconfig</td><td>16/01/2020 13:58</td><td>Archivo JavaScript</td><td>1 KB</td></tr><tr><td>channel-prefs</td><td>08/01/2020 3:00</td><td>Archivo JavaScript</td><td>1 KB</td></tr></table>	Nombre	Fecha de modifica...	Tipo	Tamaño	autoconfig	16/01/2020 13:58	Archivo JavaScript	1 KB	channel-prefs	08/01/2020 3:00	Archivo JavaScript	1 KB
Nombre	Fecha de modifica...	Tipo	Tamaño										
autoconfig	16/01/2020 13:58	Archivo JavaScript	1 KB										
channel-prefs	08/01/2020 3:00	Archivo JavaScript	1 KB										

5.5. Appliquer les paramètres de sécurité et de confidentialité

Étapes

Description

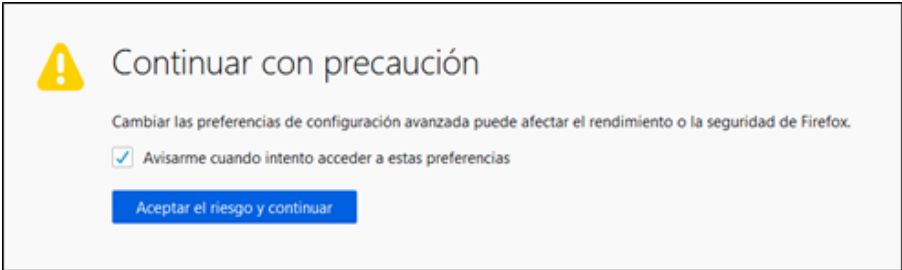
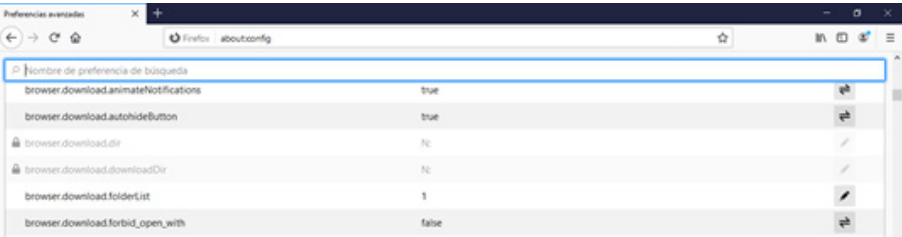
2.

The screenshot shows a Windows File Explorer window titled 'Mozilla Firefox'. The address bar indicates the path: 'Este equipo > Disco local (C:) > Archivos de programa > Mozilla Firefox'. The left sidebar shows 'Este equipo' selected. The main pane displays a list of files and folders with columns for 'Nombre', 'Fecha de modifica...', 'Tipo', and 'Tamaño'. The file 'firefox.cfg' is highlighted with a red box.

Nombre	Fecha de modifica...	Tipo	Tamaño
browser	17/01/2020 20:32	Carpeta de archivos	
defaults	17/01/2020 20:32	Carpeta de archivos	
distribution	17/01/2020 20:34	Carpeta de archivos	
fonts	17/01/2020 20:32	Carpeta de archivos	
gmp-clearkey	17/01/2020 20:32	Carpeta de archivos	
META-INF	17/01/2020 20:32	Carpeta de archivos	
uninstall	17/01/2020 20:32	Carpeta de archivos	
crashreporter	08/01/2020 3:00	Aplicación	232 KB
firefox	08/01/2020 3:00	Aplicación	555 KB
maintenanceservice	08/01/2020 3:00	Aplicación	240 KB
maintenanceservice_installer	08/01/2020 3:00	Aplicación	159 KB
minidump-analyzer	08/01/2020 3:00	Aplicación	633 KB
pingsender	08/01/2020 3:00	Aplicación	72 KB
plugin-container	08/01/2020 3:00	Aplicación	272 KB
plugin-hang-ui	08/01/2020 3:00	Aplicación	38 KB
updater	08/01/2020 3:00	Aplicación	389 KB
precomplete	08/01/2020 3:00	Archivo	4 KB
removed-files	08/01/2020 3:00	Archivo	0 KB
firefox.cfg	17/01/2020 17:00	Archivo CFG	1 KB
omni.ja	08/01/2020 3:00	Archivo JA	22.253 KB

Remarque: Les fichiers de configuration "autoconfig.js" et "firefox.cfg" se trouvent dans le dossier "Scripts" de ce guide des meilleures pratiques.

5.6 Les valeurs des directives

Étapes	Description
1.	<p>Voici les modifications de sécurité appliquées en ajoutant les fichiers <i>“autoconfig.js”</i> et <i>“firefox.cfg”</i> dans le processus de renforcement de la sécurité établi au point “4.5 Appliquer la configuration de ”.</p> <p>Dans l’éditeur de configuration (la page <i>about:config</i>), vous trouverez une liste des préférences avancées de Firefox pour vérifier les valeurs placées dans le fichier <i>“firefox.cfg”</i>.</p> <p>Pour accéder aux préférences avancées, tapez about:config et appuyez sur Entrée dans la barre d’adresse. Lorsque vous faites cela, une page d’avertissement apparaît avec un avertissement indiquant que la modification de ces paramètres avancés peut affecter les performances ou la sécurité de Firefox.</p> <p>Pour continuer, cliquez sur Accepter les risques et poursuivre.</p> <div></div>
2.	<p>En haut de la page <i>about:config</i>, vous pouvez utiliser le champ de recherche pour retrouver rapidement des préférences spécifiques.</p> <div></div>

5.6 Les valeurs des directives

Firefox est configuré pour utiliser un magasin de mots de passe avec ou sans mot de passe principal.



Firefox peut être configuré pour stocker les mots de passe des sites visités par l'utilisateur. Ces mots de passe individuels sont stockés dans un fichier et peuvent être protégés par un mot de passe principal.

Le remplissage automatique du mot de passe peut être activé lors de la visite du site web. Cette fonction peut également être utilisée pour remplir automatiquement le code d'identification d'un certificat, ce qui peut compromettre les informations.

La valeur **"signon.rememberSignons"** doit être définie à **"false"** dans le fichier **"firefox.cfg"**.

Vérifiez:

Tapez **"about:config"** dans la fenêtre du navigateur. Vérifiez que le nom de la préférence **"signon.rememberSignons"** est défini et verrouillé sur **"false"**.

5.6 Les valeurs des directives

L'assistance au remplissage des formulaires est désactivée dans Firefox.



Afin de protéger la vie privée et les données sensibles, Firefox offre la possibilité de configurer le programme de manière à ce que les données saisies dans les formulaires ne soient pas enregistrées. Ce paramètre atténue le risque qu'une page Web puisse obtenir des informations privées précédemment saisies.

La valeur "**browser.formfill.enable**" doit être définie à "false" dans le fichier "firefox.cfg".

Vérifiez:

Tapez "about:config" dans la fenêtre du navigateur. Vérifiez que le nom de la préférence "browser.formfill.enable" est défini et verrouillé sur "false".

5.6 Les valeurs des directives

Firefox est configuré pour compléter automatiquement les mots de passe.

En raison de la manière dont les informations d'identification sont stockées, il est possible pour un pirate d'accéder aux comptes des utilisateurs.

La valeur **"signon. autofillForms"** doit être définie à "false" dans le fichier "firefox.cfg".

Vérifiez:

Tapez "about:config" dans la fenêtre du navigateur. Vérifiez que le nom de la préférence "signon. autofillForms" est défini et verrouillé sur "false".



5.6 Les valeurs des directives

Les préférences de sécurité requises par Firefox ne peuvent pas être modifiées par l'utilisateur.



Le verrouillage de la configuration empêche les utilisateurs d'accéder à "about:config" et de modifier les paramètres de sécurité définis par l'administrateur système.

Vérifiez:

Tapez "about:config" dans la fenêtre du navigateur et vérifiez que les valeurs placées dans le fichier "firefox.cfg" sont marquées comme verrouillées.

5.6 Les valeurs des directives

Firefox met automatiquement à jour les add-ons et les plugins.



La définition de cette valeur sur "false" désactive toute communication avec un serveur supplémentaire pour vérifier les nouvelles versions des modules complémentaires. Les mises à jour automatiques provenant de sites non fiables exposent le navigateur à un risque pour un attaquant et peuvent neutraliser les paramètres de sécurité.

Si l'installation de modules complémentaires de navigateur est requise, il est recommandé de définir la valeur sur "true" pour éviter de perdre les derniers correctifs de sécurité de ces modules complémentaires. Il convient de s'assurer que l'installation de ces modules complémentaires et de leurs correctifs de sécurité provient de sources fiables.

La valeur "extensions.update.enabled" doit être définie à "false" dans le fichier "firefox.cfg".

Vérifiez:

Tapez "about:config" dans la fenêtre du navigateur. Vérifiez que le nom de la préférence "extensions.update.enabled" est défini et verrouillé sur "false".

5.6 Les valeurs des directives

Firefox est configuré pour se mettre à jour automatiquement.



L'autorisation de mises à jour logicielles provenant de sites non fiables peut introduire des valeurs qui invalident une installation sécurisée du navigateur avec le risque connu.

Si cette option est activée, "true", les paramètres par défaut contenant les URLs définis pour les mises à jour automatiques doivent être vérifiés, et n'autoriser que les URLs par défaut.

Si les valeurs de "app.update.url", "app.update.url.details" et "app.update.url.manual" ont été modifiées, elles doivent être restaurées à leurs valeurs par défaut.

Avec la valeur "app.update.enabled" définie sur "true", dans le fichier "firefox.cfg", vous devez effectuer les étapes indiquées dans la vérification.

Vérifiez:

Tapez "about:config" dans la fenêtre du navigateur. Vérifiez que le nom de la préférence "app.update.enabled" est défini et verrouillé sur "true".

Vérifiez que les valeurs de référence "app.update.url", "app.update.url.details" et "app.update.url.manual" contiennent une url qui pointe vers un serveur interne de confiance ou vers la configuration par défaut "Mozilla.com" ou "Mozilla.org".

Remarque: Pour désactiver les mises à jour sur Internet, définissez ces valeurs comme indiqué ci-dessous, dans le fichier "firefox.cfg":

```
lockPref("app.update.enabled", false);  
lockPref("app.update.url", "");
```

5.6 Les valeurs des directives

Firefox vérifie automatiquement la version actuelle des plugins de recherche installés.

Les mises à jour doivent être contrôlées et installées à partir de serveurs autorisés et de confiance. Ce paramètre a priorité sur les autres paramètres qui peuvent indiquer à l'application d'accéder à des URL externes.

La valeur "browser.search.update" doit être définie à "false" dans le fichier "firefox.cfg".

Vérifiez:

Tapez "about:config" dans la fenêtre du navigateur. Vérifiez que le nom de la préférence "browser.search.update" est défini et verrouillé sur "false".



5.6 Les valeurs des directives

Firefox est configuré pour demander quel certificat présenter à un site Web lorsqu'un certificat est requis.



Lorsqu'un site Web demande un certificat pour l'authentification de l'utilisateur, Firefox doit être configuré pour laisser l'utilisateur choisir le certificat à présenter. L'utilisateur se verra refuser l'accès si la gestion des certificats n'est pas configurée.

La valeur "security.default_personal_cert" doit être définie sur "Ask Every Time" dans le fichier "firefox.cfg".

Vérifiez:

Tapez "about:config" dans la fenêtre du navigateur. Vérifiez que le nom de préférence "security.default_personal_cert" est défini et verrouillé sur "Ask Every Time".

5.6 Les valeurs des directives

L'envoi d'informations d'arrière-plan à Mozilla doit être désactivé.



Aucune information technique ou autre ne doit être envoyée de notre système à Mozilla.

La valeur "datareporting.policy.dataSubmissionEnabled" doit être définie à "false" dans le fichier "firefox.cfg".

La valeur "datareporting.healthreport.service.enabled" doit être définie à "false" dans le fichier "firefox.cfg".

La valeur "datareporting.healthreport.uploadEnabled" doit être définie à "false" dans le fichier "firefox.cfg".

Vérifiez:

Tapez "about : config" dans la fenêtre du navigateur. Vérifiez que les noms de préférences "datareporting.policy.dataSubmissionEnabled", "datareporting.healthreport.service.enabled" et "datareporting.healthreport.uploadEnabled" sont définis et verrouillés sur "false".

5.6 Les valeurs des directives

L'installation d'extensions doit être désactivée.



L'installation d'extensions doit être désactivée. Une extension de navigateur est un programme qui est installé sur le navigateur et qui lui ajoute de nouvelles fonctionnalités.

Un module complémentaire interagit avec une page web et généralement avec une application tierce externe (Flash, Adobe Reader), une extension interagit avec le navigateur lui-même.

Les extensions ne sont pas intégrées dans les pages web et doivent être téléchargées et installées pour fonctionner. Les extensions permettent aux navigateurs de contourner les restrictions qui s'appliquent aux pages web.

Si un navigateur est configuré pour autoriser l'utilisation sans restriction de l'extension, des modules complémentaires peuvent être chargés et installés à partir de sources malveillantes et utilisés dans le navigateur.

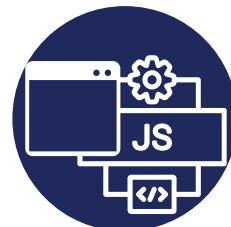
La valeur "xpinstall.enabled" doit être définie à "false" dans le fichier "firefox.cfg".

Vérifiez:

Tapez "about : config" dans la fenêtre du navigateur. Vérifiez que le nom de préférence "xpinstall.enabled" est défini et verrouillé sur "false".

5.6 Les valeurs des directives

Firefox est configuré pour permettre à JavaScript de faire apparaître (mettre devant) ou disparaître (mettre derrière) les fenêtres.



JavaScript peut modifier l'apparence du navigateur. Le fait de permettre à un site web d'utiliser JavaScript pour faire passer les fenêtres du navigateur à l'avant et/ou les renvoyer à l'arrière peut cacher une attaque. Les fenêtres du navigateur ne peuvent pas être définies comme actives via JavaScript.

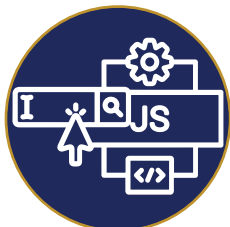
La valeur "dom.disable_window_flip" doit être définie sur "true" dans le fichier "firefox.cfg".

Vérifiez:

Tapez "about:config" dans la fenêtre du navigateur. Vérifiez que le nom de préférence "dom.disable_window_flip" est défini et verrouillé sur "true".

5.6 Les valeurs des directives

Firefox est configuré pour permettre à JavaScript de modifier le texte de la barre d'état.



JavaScript peut modifier l'apparence du navigateur. Cette action peut aider à dissimuler une attaque qui a lieu dans une fenêtre minimisée. Les auteurs de pages Web peuvent désactiver de nombreuses fonctions liées à l'ouverture d'une fenêtre pop-up.

Le réglage de cette préférence sur "true" remplace le réglage de l'auteur Web et garantit que la barre d'état est activée et présente dans toute fenêtre contextuelle. Ce paramètre empêche la barre d'état d'être masquée dans toute fenêtre de navigateur.

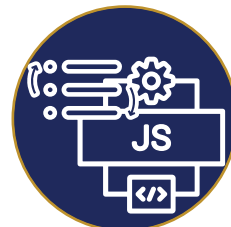
La valeur "dom.disable_window_open_feature.status" doit être définie à "true" dans le fichier "firefox.cfg".

Vérifiez:

Tapez "about:config" dans la fenêtre du navigateur. Vérifiez que le nom de préférence "dom.disable_window_open_feature.status" est défini et verrouillé sur "true".

5.6 Les valeurs des directives

Firefox est configuré pour permettre à JavaScript de désactiver ou de remplacer les menus contextuels.



Un menu contextuel (également connu sous le nom de menu contextuel) est souvent utilisé dans une interface utilisateur graphique (GUI). Ce menu apparaît après une interaction de l'utilisateur (par exemple, un clic droit de la souris). Un menu contextuel offre un ensemble limité d'options disponibles dans l'état ou le contexte actuel du système d'exploitation ou de l'application.

Un site web peut exécuter du JavaScript pour apporter des modifications à ces menus contextuels, ce qui peut aider à dissimuler une attaque. Cette préférence doit être définie sur "false" afin que les pages Web ne puissent pas apporter de modifications au menu contextuel.

La valeur "dom.event.contextmenu.enabled" doit être définie à "false" dans le fichier "firefox.cfg".

Vérifiez:

Tapez "about:config" dans la fenêtre du navigateur. Vérifiez que le nom de la préférence "dom.event.contextmenu.enabled" est défini et verrouillé sur "false".

5.6 Les valeurs des directives



Firefox n'est pas configuré pour afficher un message d'invite à l'utilisateur avant de télécharger et d'ouvrir les différents types de fichiers.

Les nouveaux types de fichiers ne peuvent pas être ajoutés directement à la liste des compléments ou des applications d'aide. Les fichiers avec ces extensions ne pourront pas utiliser Firefox directement, mais utiliseront des applications externes pour ouvrir les fichiers.

Les applications externes sont configurées après qu'une action de téléchargement d'un type de fichier non stocké dans le navigateur a été définie. À ce stade, vous sélectionnez l'action à effectuer, l'affectation d'une application externe pour ouvrir le fichier ou l'option pour enregistrer le fichier à télécharger. Une fois l'option sélectionnée, et tant que l'option Faire cela automatiquement pour les fichiers comme celui-ci à partir de maintenant est cochée, cela sera fait automatiquement pour les futurs téléchargements du même type de fichier.

Cette action génère une entrée pour ce type de fichier dans la liste des plugins et permettra ainsi l'ouverture automatique de ce type de fichier à l'avenir.

Ce paramètre peut constituer un problème de sécurité. Les nouveaux types de fichiers ne doivent pas pouvoir être ajoutés directement à la liste des modules complémentaires de l'application afin d'éviter toute utilisation malveillante éventuelle.

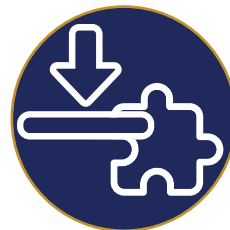
La valeur "plugin.disable_full_full_page_plugin_for_types" doit être définie comme "true" dans le fichier "firefox.cfg".

Vérifiez:

Tapez "about:config" dans la fenêtre du navigateur. Vérifiez que le nom de préférence "plugin.disable_full_full_page_plugin_for_types" est défini et verrouillé sur "true".

5.6 Les valeurs des directives

Le plug-in des contrôles ActiveX est installé sur Firefox.



Lorsqu'un contrôle ActiveX est référencé dans un document HTML, MS Windows vérifie si le contrôle réside déjà sur la machine cliente. Sinon, le contrôle peut être téléchargé à partir d'un site web distant. Cela fournit une méthode de livraison automatisée pour le code mobile.

Le support des contrôles ActiveX et des plug-ins ne doit pas être présent ou activé.

Vérifiez:

Tapez "about:plugins" dans la fenêtre du navigateur. Vérifiez qu'il n'y a pas de plug-in ActiveX. Dans le cas contraire, supprimez ou désinstallez.

5.6 Les valeurs des directives

Le protocole shell réseau est activé dans Firefox.



Bien que les versions actuelles de Firefox aient cette valeur désactivée par défaut, l'utilisation de cette option peut être dangereuse. Cela permettrait au navigateur d'accéder au shell de Windows.

La valeur "network.protocol-handler.external.shell" doit être définie à "false" dans le fichier "firefox.cfg".

Vérifiez:

Tapez "about:config" dans la fenêtre du navigateur. Vérifiez que le nom de préférence "network.protocol-handler.external.shell" est défini et verrouillé sur "false".

5.6 Les valeurs des directives

Firefox n'est pas configuré pour fournir des avertissements lorsqu'un utilisateur passe d'une page sécurisée (SSL activé) à une page non sécurisée.



Les utilisateurs peuvent ne pas savoir qu'ils passent d'une page précédemment sécurisée à une page actuelle non sécurisée.

La valeur "security.warn_leaving_secure" doit être définie à "true" dans le fichier "firefox.cfg".

Vérifiez:

Tapez "about:config" dans la fenêtre du navigateur. Vérifiez que le nom de préférence "security.warn_leaving_secure" est défini et verrouillé sur "true".

5.6 Les valeurs des directives

Firefox n'est pas configuré pour bloquer les pop-ups.



Les fenêtres pop-up peuvent être utilisées pour lancer une attaque dans une nouvelle fenêtre du navigateur avec des paramètres modifiés. Ce paramètre bloque les fenêtres pop-up créées pendant le chargement de la page.

La valeur " `dom.disable_window_open_feature.status` " doit être définie comme " `true` " dans le fichier " `firefox.cfg` ".

Vérifiez:

Tapez "about:config" dans la fenêtre du navigateur. Vérifiez que le nom de préférence "dom.disable_window_open_feature.status" est défini et verrouillé sur "true".

5.6 Les valeurs des directives

Firefox est configuré pour autoriser le JavaScript à déplacer ou redimensionner les fenêtres.



JavaScript peut modifier l'apparence du navigateur. Cette activité peut aider à dissimuler une attaque qui se déroule dans une fenêtre d'arrière-plan minimisée. Les paramètres du navigateur doivent être réglés pour empêcher les scripts des sites Web visités de déplacer et de redimensionner les fenêtres du navigateur.

La valeur "dom.disable_window_flip" doit être définie sur "true" dans le fichier "firefox.cfg".

Vérifiez:

Tapez "about:config" dans la fenêtre du navigateur. Vérifiez que le nom de préférence "dom.disable_window_flip" est défini et verrouillé sur "true".

5.6 Les valeurs des directives

Firefox doit être configuré pour n'autoriser que TLS.



L'utilisation de protocoles sécurisés avec des versions antérieures à TLS 1.1 met la sécurité en danger. Les anciens protocoles SSL 2.0, SSL 3.0 et TLS 1.0 contiennent un certain nombre de failles de sécurité qui peuvent compromettre le navigateur. Ces protocoles doivent être désactivés en fonction des besoins de l'infrastructure du réseau.

Il est recommandé de définir "security.tls.version.min" avec la valeur "2" pour l'utilisation du protocole TLS 1.1 comme valeur minimale.

Il est recommandé de définir "security.tls.version.max" avec la valeur "3" pour l'utilisation du protocole TLS 1.2 comme valeur maximale.

Ces valeurs doivent apparaître dans le fichier "firefox.cfg".

Vérifiez:

Tapez "about:config" dans la fenêtre du navigateur et vérifiez les noms préférés suivants:



"security.tls.version.min" fixé à "2".



"security.tls.version.max" fixé à "3".

5.6 Les valeurs des directives

Firefox exécute ou télécharge automatiquement les types MIME qui ne sont pas autorisés pour le téléchargement automatique.



L'action par défaut, pour les types de fichiers pour lesquels un module complémentaire est installé, consiste à télécharger et à exécuter automatiquement le fichier en utilisant le module complémentaire associé. Firefox vous permet de modifier l'action de téléchargement spécifiée afin que le fichier soit ouvert avec une application externe sélectionnée ou enregistré sur le disque.

Affichez la liste des plug-ins de navigateur installés et des types MIME associés en saisissant "about:plugins" dans la barre d'adresse. Lorsque vous cliquez sur un lien pour télécharger un fichier, le type MIME détermine l'action de Firefox.

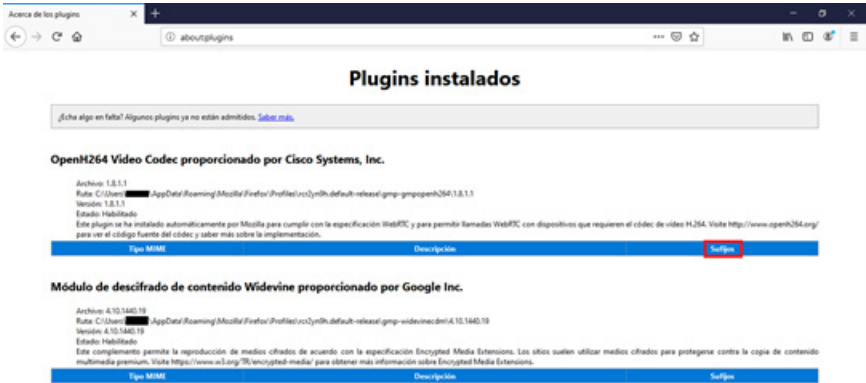

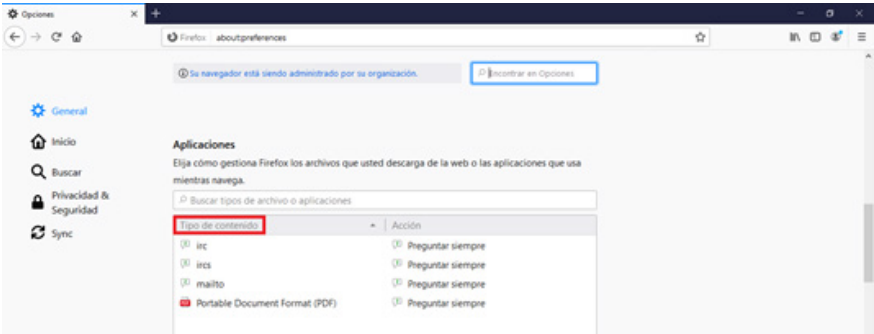
Il se peut que vous ayez déjà installé un plug-in qui se chargera automatiquement du téléchargement, tel que Windows Media Player ou QuickTime. D'autres fois, vous verrez apparaître une boîte de dialogue vous demandant si vous voulez enregistrer le fichier ou l'ouvrir avec une application spécifique.

Lorsque vous demandez à Firefox d'ouvrir ou d'enregistrer le fichier et que vous cochez également l'option "Faire cela automatiquement pour les fichiers comme celui-ci à partir de maintenant", une entrée pour ce type de fichier apparaît dans le volet Applications de Firefox.

Vérifiez:

Utilisez l'option A ou B pour vérifier si les extensions suivantes apparaissent dans les paramètres de votre navigateur : HTA, JSE, JS, MOCHA, SHS, VBE, VBS, SCT, WSC. Par défaut, la plupart de ces extensions n'apparaîtront pas dans la liste de Firefox.

5.6 Les valeurs des directives

Option	Description
<p>A.</p>	<p>Sous “about:plugins”, plug-in installé, vous devez inspecter les entrées de la colonne Suffixe. Dans cette colonne, vous ne devriez pas trouver les extensions mentionnées ci-dessus. Si vous en trouvez un, vérifiez qu’il n’est pas associé à une application exécutant du code.</p> <p>Il existe des applications telles que Notepad.exe, qui n’exécutent pas de code, mais qui peuvent être associées aux extensions mentionnées.</p> <p>Supprimez toute extension non autorisée de la liste.</p> 
<p>B.</p>	<p>Cliquez sur le  bouton de menu, cliquez sur “Options” et recherchez les extensions mentionnées dans la colonne “Type de contenu” sous “Applications”.</p> <p>Il est recommandé que les extensions mentionnées ci-dessus, montrent dans la colonne “Action” les options “Enregistrer le fichier” ou “Toujours demander”. Une autre possibilité est qu’il soit associé à une application qui n’exécute pas de code (par exemple, Notepad).</p> <p>Si vous trouvez que l’une des extensions ci-dessus dans la colonne “Action” est associée à une application qui peut exécuter le code, il est alors recommandé de la supprimer de la liste.</p> 

5.6 Les valeurs des directives

Firefox n'est pas configuré pour utiliser le magasin de certificats de Windows.



À partir de Firefox 49, une nouvelle option a été incluse qui permet à Firefox de faire confiance aux autorités racine dans le magasin de certificats de Windows. Cela signifie que les certificats peuvent être déployés normalement par le biais de la stratégie de groupe et que Firefox fera confiance aux mêmes autorités racinaires qu'Internet Explorer.

Cette fonction est désactivée par défaut.

Pour activer ce paramètre, vous devez créer une nouvelle entrée, avec la valeur "security.enterprise_roots.enabled" définie sur "true", dans le fichier "firefox.cfg".

Vérifiez:

Tapez "about:config" dans la fenêtre du navigateur. Vérifiez que le nom de préférence "security.enterprise_roots.enabled" est configuré et verrouillé à l'ensemble des options.

5.6 Les valeurs des directives

Firefox est configuré pour autoriser la complétion automatique.



Pour protéger nos informations, Firefox offre la possibilité de se configurer pour que les données saisies dans les formulaires ne soient pas enregistrées. Cela réduit le risque qu'un site web obtienne des informations privées à partir de ces informations enregistrées.

La valeur "browser.formfill.enable" doit être définie à "false" dans le fichier "firefox.cfg".

Vérifiez:

Tapez "about:config" dans la fenêtre du navigateur. Vérifiez que le nom de la préférence "browser.formfill.enable" est défini et verrouillé sur "false".

5.6 Les valeurs des directives

Firefox est configuré pour montrer notre véritable IP lors de la navigation.



La désactivation du protocole WebRTC (Web Real-Time Communication) vous permet d'améliorer considérablement votre vie privée. Ce protocole cache plusieurs problèmes de confidentialité assez graves, problèmes qui peuvent être omis, par exemple, en filtrant l'adresse IP réelle lors de la navigation via un VPN.

Toutefois, la désactivation de ce protocole peut entraîner l'arrêt du fonctionnement de certaines applications et outils Web qui en dépendent. Des applications telles que WhatsApp Web cessent de fonctionner.

Il existe des sites web qui indiquent si le navigateur laisse échapper des informations personnelles par le biais de ce protocole.



<https://ipleak.net/>



<https://browserleaks.com/>

La valeur "media.peerconnection.enabled" doit être définie à "false" dans le fichier "firefox.cfg".

Vérifiez:

Tapez "about:config" dans la fenêtre du navigateur. Vérifiez que le nom de préférence "media.peerconnection.enabled" est défini et verrouillé sur "false".

5.6 Les valeurs des directives

Supprimez les fichiers générés pendant la navigation lors de la fermeture du navigateur.



Certaines configurations doivent être définies pour que, lorsque la navigation se termine et que le navigateur est fermé, les fichiers générés par le navigateur pendant son fonctionnement soient supprimés.

Cela permet de charger, lors de la prochaine visite du site, les dernières versions des pages visitées, ainsi que les paramètres du site, améliorant ainsi la sécurité globale de la navigation.

Pour effectuer cette opération, les propriétés suivantes doivent être définies dans le fichier de configuration :











- `privacy.sanitize.sanitizeOnShutdown`
- `privacy.clearOnShutdown.cache`
- `privacy.clearOnShutdown.cookies`
- `privacy.clearOnShutdown.downloads`
- `privacy.clearOnShutdown.formdata`
- `privacy.clearOnShutdown.history`
- `privacy.clearOnShutdown.offlineApps`
- `privacy.clearOnShutdown.openWindows`
- `privacy.clearOnShutdown.sessions`
- `privacy.clearOnShutdown.siteSettings`

Dans les organisations qui doivent conserver l'historique de navigation, la préférence "`privacy.clearOnShutdown.history`" doit être définie pour permettre la mémorisation de l'historique de navigation, en fixant la valeur à "`false`" pour que l'historique ne soit pas supprimé à la fermeture du navigateur.

5.6 Les valeurs des directives

Vérifiez:

Tapez "about:config" dans la fenêtre du navigateur. Vérifiez que les noms de préférences suivants sont définis et verrouillés sur "true":

-  `privacy.sanitize.sanitizeOnShutdown`
-  `privacy.clearOnShutdown.cache`
-  `privacy.clearOnShutdown.cookies`
-  `privacy.clearOnShutdown.downloads`
-  `privacy.clearOnShutdown.formdata`
-  `privacy.clearOnShutdown.history`
-  `privacy.clearOnShutdown.offlineApps`
-  `privacy.clearOnShutdown.openWindows`
-  `privacy.clearOnShutdown.sessions`
-  `privacy.clearOnShutdown.siteSettingsite`

5.6 Les valeurs des directives

Désactivez la fonction de synchronisation du compte Firefox.



Firefox Account, anciennement connu sous le nom de Firefox Sync, est une fonctionnalité intégrée au navigateur qui permet aux utilisateurs de synchroniser automatiquement divers éléments tels que les signets, les onglets ouverts, les mots de passe et les modules complémentaires.

Si vous ne souhaitez pas utiliser la synchronisation et l'installation de tout ce qui est configuré dans un compte Firefox et éviter ainsi les problèmes de confidentialité et de sécurité, vous devez désactiver cette fonctionnalité du navigateur.

La valeur "identity.fxaccounts.enabled" doit être définie à "false" dans le fichier "firefox.cfg".

Vérifiez:

Tapez "about : config" dans la fenêtre du navigateur. Vérifiez que le nom de préférence "identity.fxaccounts.enabled" est défini et verrouillé sur "false".

5.6 Les valeurs des directives

Désactiver Pocket dans Firefox.

Pocket est une fonction qui permet aux utilisateurs d'enregistrer tout type de contenu web pour le consulter ultérieurement.

Pour les organisations qui préfèrent activer la fonctionnalité Pocket, la préférence "extensions.pocket.enabled" doit être définie sur "true".

La valeur "extensions.pocket.enabled" doit être définie à "false" dans le fichier "firefox.cfg".

Vérifiez:

Tapez "about:config" dans la fenêtre du navigateur. Vérifiez que le nom de préférence "extensions.pocket.enabled" est défini et verrouillé sur "false"



6. Liste de contrôle (évaluation)

Criticité	Vérification
Haut	Mozilla Firefox doit avoir installé les dernières mises à jour logicielles relatives à la sécurité.
Haut	Mozilla Firefox est configuré pour utiliser un coffre-fort de mots de passe avec ou sans mot de passe principal.
Médias	L'option de prise en charge du remplissage de formulaires de Mozilla Firefox est désactivée.
Médias	Mozilla Firefox est configuré pour remplir automatiquement les mots de passe.
Médias	Les préférences de sécurité requises par Mozilla Firefox ne peuvent pas être modifiées par l'utilisateur.
Médias	Mozilla Firefox met automatiquement à jour les add-ons et plugins
Médias	Mozilla Firefox est configuré pour se mettre à jour automatiquement
Médias	Mozilla Firefox vérifie automatiquement les versions mises à jour des plugins de recherche installés.
Médias	Mozilla Firefox est configuré pour demander quel certificat présenter à un site web lorsqu'un certificat est requis.
Médias	L'envoi d'informations d'arrière-plan à Mozilla Firefox doit être désactivé.
Médias	L'installation d'extensions doit être désactivée.
Médias	Mozilla Firefox est configuré pour permettre à JavaScript de faire apparaître (mettre devant) ou de faire disparaître (mettre derrière) des fenêtres.
Médias	Mozilla Firefox est configuré pour permettre à JavaScript de modifier le texte de la barre d'état.
Médias	Mozilla Firefox est configuré pour permettre à JavaScript de désactiver ou de remplacer les menus contextuels.

6. Lista de comprobación (assessment)

Criticité	Vérification
Médias	Mozilla Firefox n'est pas configuré pour afficher un message d'invite à l'utilisateur avant de télécharger et d'ouvrir différents types de fichiers.
Médias	Le plug-in pour les contrôles ActiveX est installé sur Mozilla Firefox.
Médias	Le protocole shell réseau est activé dans Mozilla Firefox.
Médias	Mozilla Firefox n'est pas configuré pour fournir des avertissements lorsqu'un utilisateur passe d'une page sécurisée (SSL activé) à une page non sécurisée.
Médias	Mozilla Firefox n'est pas configuré pour bloquer les fenêtres pop-up.
Médias	Mozilla Firefox est configuré pour permettre à JavaScript de déplacer ou de redimensionner les fenêtres.
Médias	Mozilla Firefox doit être configuré pour n'autoriser que TLS.
Médias	Mozilla Firefox exécute ou télécharge automatiquement les types MIME qui ne sont pas autorisés pour le téléchargement automatique.
Médias	Mozilla Firefox n'est pas configuré pour utiliser le magasin de certificats de Windows.
Médias	Mozilla Firefox est configuré pour autoriser la complétion automatique.
Médias	Mozilla Firefox est configuré pour montrer notre véritable IP lors de la navigation.

7. Décalogue de recommandations

Voici dix (10)
recommandations de
sécurité pour *Mozilla
Firefox*



Décalogue de sécurité pour Mozilla Firefox



Utilisez toujours la dernière version de Mozilla Firefox.



En cas d'installation de modules complémentaires, il est recommandé de vérifier qu'elle est effectuée à partir de sources fiables.



Il est conseillé d'examiner toutes les fonctions de sécurité du logiciel, car elles offrent une meilleure défense contre les attaques.



Il est recommandé de ne pas stocker les mots de passe par défaut et d'utiliser plutôt d'autres applications qui mettent en œuvre un cryptage fort pour stocker vos mots de passe en toute sécurité.



Il est recommandé de regarder le bouton d'identité du site (un cadenas dans la barre d'adresse, à gauche de celle-ci) pour savoir rapidement et facilement si la connexion à la page est cryptée et, dans certains cas, qui en est le propriétaire. Ces informations aident à la détection des pages malveillantes.



Il est recommandé de toujours utiliser https, en particulier lorsque des données personnelles sont utilisées pour sécuriser les communications de bout en bout.



L'utilisation du logiciel PGP pour envoyer des informations personnelles cryptées est recommandée comme mesure de sécurité supplémentaire, même en cas d'utilisation de protocoles sécurisés tels que https.



L'utilisation d'une authentification à deux facteurs est recommandée lors de l'utilisation de services en ligne. Lorsque vous configurez le service pour envoyer un code PIN au téléphone mobile. Cela ajoute une couche supplémentaire de sécurité aux comptes.



Il est recommandé de supprimer vos cookies pour empêcher certains sites web de suivre vos habitudes de recherche et pour protéger votre vie privée.



Nous vous recommandons de vider votre cache et de supprimer les fichiers Internet temporaires pour résoudre les problèmes courants liés aux sites Web.

Annexe A.

Fichier de configuration de la sécurité

Pour faciliter l'application du contrôle de sécurité sur Mozilla Firefox, un dossier contenant les fichiers nécessaires à la sécurisation des informations sur un ordinateur est inclus dans ce document.

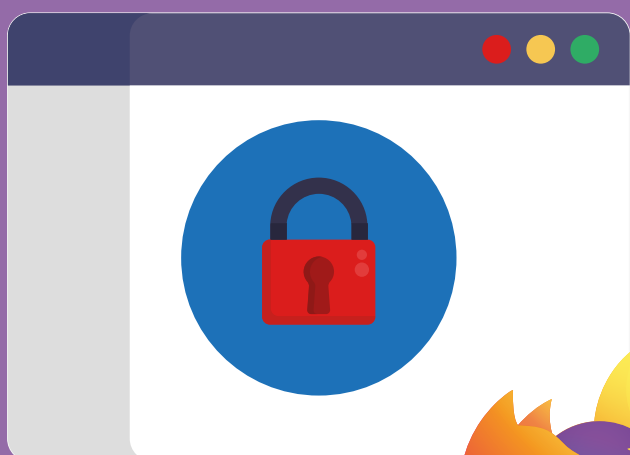
Les fichiers inclus dans le dossier **"Scripts"** sont énumérés ci-dessous.



autoconfig.js



firefox.cfg



www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es