FINANCES PUBLIQUES

J. 20 1374

CONCOURS EXTERNE POUR L'ACCÈS AU GRADE D'INSPECTEUR DES FINANCES PUBLIQUES AFFECTÉ AU TRAITEMENT DE L'INFORMATION EN QUALITÉ DE PROGRAMMEUR DE SYSTÈME D'EXPLOITATION

ANNÉE 2021

_____

ÉPREUVE ÉCRITE D'ADMISSION N° 3

Durée : 1 heure 30 – Coefficient : 1

_____

Version anglaise à partir d'un texte issu d'une revue ou d'une documentation informatique

_____

Recommandations importantes

Le candidat trouvera au verso la manière de servir la copie dédiée.

Sous peine d'annulation, en dehors du volet rabattable d'en-tête, les copies doivent être totalement anonymes et ne comporter aucun élément d'identification tels que nom, prénom, signature, paraphe, localisation, initiale, numéro ou toute autre indication, même fictive, étrangère au traitement du sujet.

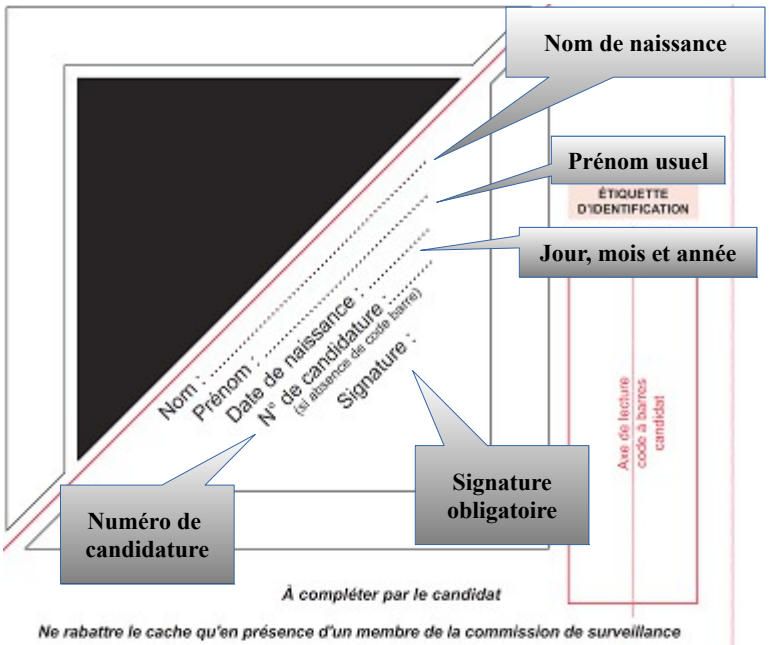
Sur les copies, les candidats devront écrire et souligner si nécessaire au stylo bille, plume ou feutre de couleur noire ou bleue uniquement. De même, l'utilisation de crayon surligneur est interdite.

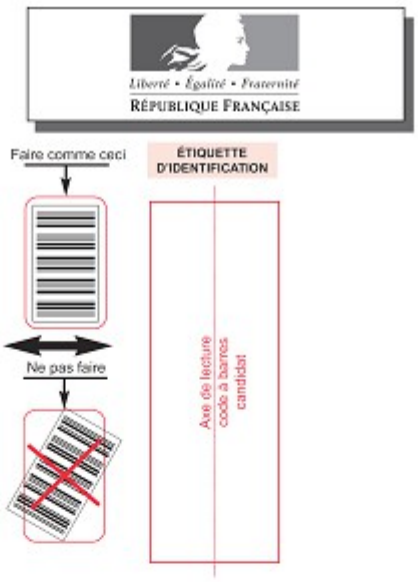
Il devra obligatoirement se conformer aux directives données.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Tournez la page S.V.P.

Le candidat complétera l'intérieur du volet rabattable des informations demandées et se conformera aux instructions données





Concours externe - interne - professionnel - ou examen professionnel (1)
(1) Rayer les mentions inutiles

Externe

Pour l'emploi de : **Inspecteur des Finances Publiques affecté au traitement de l'information en qualité de programmeur de système d'exploitation**

Épreuve n° : **3**

Matière : **Version anglaise**

Date : **19 11 20 20**

Nombre d'intercalaires supplémentaires :

Préciser éventuellement le nombre d'intercalaires supplémentaires

À L'ATTENTION DU CANDIDAT

En dehors de la zone d'identification rabattable, les copies doivent être totalement anonymes et ne comporter aucun élément d'identification tel que nom, prénom, signature, paraphe, localisation, initiale, numéro, ou toute autre indication même fictive étrangère au traitement du sujet.

Il est demandé aux candidats d'écrire et de souligner si nécessaire au stylo bille, plume ou feutre, de couleur noire ou bleue uniquement. Une autre couleur pourrait être considérée comme un signe distinctif par le jury, auquel cas la note de zéro serait attribuée. De même, l'utilisation de crayon surligneur est interdite.

Les étiquettes d'identification codes à barres, destinées à permettre à l'administration d'identifier votre copie, ne doivent être détachées et collées dans les deux cadres prévus à cet effet qu'en présence d'un membre de la commission de surveillance.

Suivre les instructions données pour les étiquettes d'identification

NOTE / 20 ,

RÉSERVÉ À L'ADMINISTRATION

À L'ATTENTION DU CORRECTEUR

Pour remplir ce document :
Utilisez un stylo ou une pointe feutre de couleur NOIRE ou BLEUE.

EXEMPLE DE MARQUAGE : Faire comme ceci — Ne pas faire

Pour porter votre note, cochez les gélules correspondantes.

Reportez la note dans les zones NOTE / 20 et dans le cadre A

En cas d'erreur de codification dans le report des notes cochez la case erreur et reportez la note dans le cadre B.

Cadre A réservé à la notation		
20	19	18
17	16	15
14	13	12
11	10	09
08	07	06
05	04	03
02	01	00
Décimales		
,00	,25	,50 ,75

Cadre B réservé à la notation rectificative		
20	19	18
17	16	15
14	13	12
11	10	09
08	07	06
05	04	03
02	01	00
Décimales		
,00	,25	,50 ,75
Erreur		

NOTE / 20 ,

EN AUCUN CAS, LE CANDIDAT NE FERMERA LE VOLET RABATTABLE AVANT D'Y AVOIR ÉTÉ AUTORISÉ PAR LA COMMISSION DE SURVEILLANCE

FINANCES PUBLIQUES

SUJET

Code matière : 051

Les candidates et les candidats peuvent avoir à leur disposition sur la table de concours le matériel d'écriture, une règle, un correcteur, des surligneurs.

Cybercriminal group mails malicious USB dongles to targeted companies

S*hown as a proof-of-concept in 2014, this is the first known use of the BadUSB exploit in the wild.*

Security researchers have come across an attack where an USB dongle designed to surreptitiously behave like a keyboard was mailed to a company under the guise of a Best Buy gift card. This technique has been used by security professionals during physical penetration testing engagements in the past, but it has very rarely been observed in the wild. This time it's a known sophisticated cybercriminal group who is likely behind it.

The attack was analyzed and disclosed by security researchers from Trustwave SpiderLabs, who learned about it from the business associate of one of their team members. Ziv Mador, vice president for security research Trustwave SpiderLabs, tells CSO that a US company in the hospitality sector received the USB sometime in mid-February.

The package contained an official-looking letter with Best Buy's logo and other branding elements informing the recipient that they've received a $50 gift card for being a regular customer. "You can spend it on any product from the list of items presented on an USB stick," the letter read. Fortunately, the USB dongle was never inserted into any computers and was passed along for analysis, because the person who received it had security training.

The BadUSB

Researchers traced the USB dongle model to a Taiwanese website where it's being sold for the equivalent of $7 under the name BadUSB Leonardo USB ATMEGA32U4. In 2014, at the Black Hat USA security conference, a team of researchers from Berlin-based Security Research Labs (SRLabs) demonstrated that the firmware of many USB dongles can be reprogrammed so that, when inserted in a computer, it reports that it's actually a keyboard and starts sending commands that could be used to deploy malware. The researchers dubbed this attack BadUSB and it's different then just putting malware on an USB stick and relying on the user to open it.

The Leonardo USB device that Trustwave received and analyzed has an Arduino ATMEGA32U4 microcontroller inside which was programmed to act as a virtual keyboard and execute an obfuscated PowerShell script via the command line. The script reaches out to a domain set up by the attackers and downloads a secondary PowerShell payload that then deploys a third JavaScript-based payload [...].

This third JavaScript payload generates a unique identifier for the computer and registers it to a remote command-and-control server. It then receives additional obfuscated JavaScript code from the server which it executes. The goal of this fourth payload is to gather information about the system, such as the domain name, time zone, language, OS and hardware information, a list of running processes [...].

***IT World*, March 27, 2020**