Le correcteur orthographique de Chrome et Edge fait fuiter vos mots de passe

20 septembre 2022 à 10:45

Le vérificateur d’orthographe de Microsoft Edge et le correcteur orthographique amélioré de Chrome envoient les données sensibles que vous saisissez, y compris vos mots de passe, sur les serveurs de Google et Microsoft.

L’équipe de chercheurs en sécurité d’Otto-JS a découvert que le Rédacteur Microsoft sur Microsoft Edge et le correcteur orthographique amélioré intégré à Google Chrome partagent vos données personnelles sur les serveurs de Google et de Microsoft.

Concrètement, tous les contenus entrés dans un champ de texte pouvant être analysés par ces correcteurs orthographiques, qu’il s’agisse d’une page de connexion ou d’un formulaire, sont envoyés aux deux géants américains. Cela peut inclure les noms, prénoms, adresses e-mail, date de naissance, numéro de sécurité sociale, etc. Tous les champs de texte qui peuvent être analysés par ces correcteurs orthographiques sont concernés. Si cela n’est qu’à moitié surprenant, la suite s’avère plus effrayante. En effet, l’équipe d’Otto-JS a trouvé bien pire.

En testant le comportement de leurs scripts, les dirigeants de l’entreprise ont découvert qu’en cliquant sur le bouton pour afficher le mot de passe qu’ils venaient de saisir, que celui-ci était également envoyé sur les serveurs de Google et Microsoft.

« Ce qui est préoccupant, c’est la facilité d’activation de ces fonctionnalités et le fait que la plupart des utilisateurs les activeront sans vraiment se rendre compte de ce qui se passe en arrière-plan. » a indiqué le cofondateur d’Otto-JS dans le communiqué publié par l’entreprise.

En effet, si le Rédacteur Microsoft est une extension qui doit être volontairement installée par l’utilisateur dans Edge, ce n’est pas le cas du correcteur orthographique amélioré de Chrome qui est nativement intégré dans le navigateur.

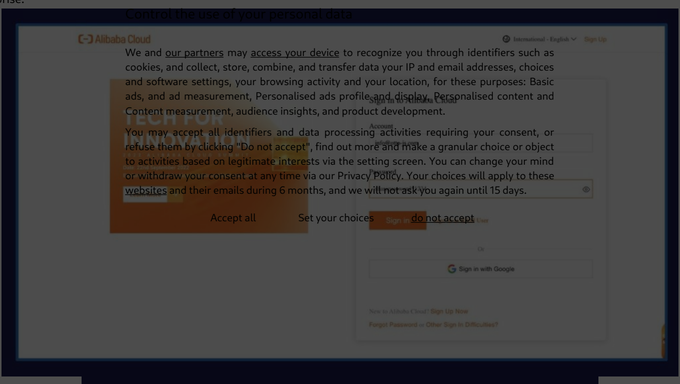
Pour illustrer le danger que peuvent représenter ces extensions, l’équipe d’Otto-JS a fait une démonstration éloquente. Les captures d’écran publiées par l’entreprise montrent ainsi que lorsqu’un utilisateur qui se connecte à Alibaba Cloud, son mot de passe est envoyé sur les serveurs de Google. Or le service n’a rien à voir avec Google ni Microsoft. Cette brèche, nommée « Spell-jacking » par Otto-JS, est transposable à n’importe quelle infrastructure clou ou réseau interne d’entreprise.

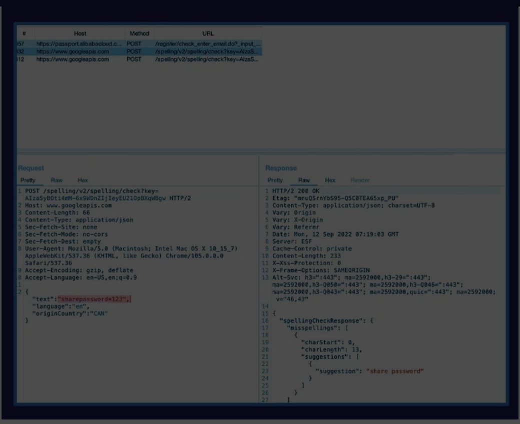
Control the use of your personal data

We and our partners may access your device to recognize you through identifiers such as cookies, and collect, store, combine, and transfer data your IP and email addresses, choices and software settings, your browsing activity and your location, for these purposes: Basic ads, and ad measurement, Personalised ads profile and display, Personalised content and Content measurement, audience insights, and product development.

You may accept all identifiers and data processing activities requiring your consent, or refuse them by clicking "Do not accept", find out more and make a granular choice or object to activities based on legitimate interests via the setting screen. You can change your mind or withdraw your consent at any time via our Privacy Policy. Your choices will apply to these websites and their emails during 6 months, and we will not ask you again until 15 days.

Accept all Set your choices do not accept





#	Host	Method	URL
57	https://passport.alibabacloud.c...	POST	/register/check_enter_email.do?_input_...
32	https://www.googleapis.com	POST	/spelling/v2/spelling/check?key=AlzaS...
12	https://www.googleapis.com	POST	/spelling/v2/spelling/check?key=AlzaS...

Request

Pretty Raw Hex

```
POST /spelling/v2/spelling/check?key=
AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw HTTP/2
Host: www.googleapis.com
Content-Length: 66
Content-Type: application/json
Sec-Fetch-Site: none
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: empty
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0
Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

{
  "text":"sharepassword*123",
  "language":"en",
  "originCountry":"CAN"
}
```

Response

Pretty Raw Hex Render

```
HTTP/2 200 OK
Etag: "mnuQSrnYbS95-Q5C0TEA65xp_PU"
Content-Type: application/json; charset=UTF-8
Vary: Origin
Vary: X-Origin
Vary: Referer
Date: Mon, 12 Sep 2022 07:19:03 GMT
Server: ESF
Cache-Control: private
Content-Length: 233
X-Xss-Protection: 0
X-Frame-Options: SAMEORIGIN
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443";
ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443";
ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000;
 v="46,43"

{
  "spellingCheckResponse": {
    "misspellings": [
      {
        "charStart": 0,
        "charLength": 13,
        "suggestions": [
          {
            "suggestion": "share password"
          }
        ]
      }
    ]
```

Otto-JS, qui a dévoilé l’existence de cette brèche à plusieurs géants du secteur, a déjà permis à plusieurs d’entre eux de corriger le tir. C’est le cas, par exemple, des équipes en charge de la sécurité d’Amazon Web Services ou encore du gestionnaire de mots de passe LastPass. Leurs équipes de sécurité ont corrigé fissa le code de leur application afin d’empêcher les correcteurs orthographiques de venir analyser les champs de texte contenant des données sensibles.

Source : Otto-JS

Geoffroy Ondet
Journaliste