

## Déclaration de l'ENISA quant à la récente faille de sécurité d'Internet Explorer

Suite aux messages d'avertissement que Microsoft a publiés dimanche quant à l'exploitation d'une faille non identifiée au sein de toutes les versions prises en charge par Internet Explorer (IE) pouvant les affecter et par ailleurs secrètement pirater les ordinateurs vulnérables, l'ENISA commente ;

- Pour clarification ; l'ENISA n'est pas une CERT opérationnelle, mais un [organisme d'experts](#) pouvant toutefois commenter la situation et en fournir une brève analyse ;
- Ceci est une « attaque jour zéro » lancée dans la nature majeure pour la société, qui prouve que la sécurité informatique ne peut être assurée à 100 % et combien la société peut être vulnérable si ces menaces ne sont pas prises en compte dès le départ. Nous préconisons donc une sécurité dès le stade de conception des logiciels selon les branches industrielles.
- Cet incident est une menace importante pour les utilisateurs d'Internet Explorer puisqu'il n'existe pas encore de solution toute prête ou de « patches » pouvant corriger le problème.
- Les utilisateurs souhaitant éviter le risque susmentionné devraient utiliser temporairement un autre navigateur jusqu'à ce que la faille de sécurité soit corrigée.
- Les utilisateurs sont appelés à veiller à ce que leurs systèmes informatiques soient outillés de patches et actualisés.
- De nombreux utilisateurs ont souvent deux navigateurs installés et devraient donc aisément pouvoir changer. Dans le cas contraire, ils ont désormais une bonne raison d'en choisir un autre, afin de pouvoir faire face à ces besoins.
- S'ils ne peuvent pas installer de deuxième navigateur, les utilisateurs d'Internet Explorer devraient s'assurer que les versions 4.1 et 5.0 de l'utilitaire de sécurité EMET (Enhanced Mitigation Experience Toolkit) soient installées sur leur ordinateur, que les mesures d'atténuation soient autorisées et que VML et Flash soient bloqués.
- Le mode protégé amélioré (EPM) d'Internet Explorer devrait être activé. Le mode EPM a été introduit dans IE10.
- Les utilisateurs devraient toujours naviguer sur Internet avec un compte en mode utilisateur limité et non pas administrateur.
- Un des problèmes majeurs est que les utilisateurs de Windows XP seront exposés à cette faille de sécurité puisqu'aucun patch ne sera proposé pour XP (arrivé en fin de vie).

L'ENISA est le centre d'expertise pour les questions de sécurité des réseaux et de l'information en Europe

Sécuriser la société de l'information en Europe

L'Agence européenne en charge de la sécurité des réseaux et de l'information

29/04/2014

EPR10/15

[www.enisa.europa.eu](http://www.enisa.europa.eu)

- Cette faille affecte près de 26 % de l'ensemble des navigateurs et souligne ainsi le degré d'importance que revêt la cybersécurité aujourd'hui pour notre société et notre économie.
- Selon l'entreprise de sécurité informatique FireEye, un groupe de cybercriminels connu des autorités est déjà en train de conduire des attaques ciblées contre des individus privés ainsi que des organisations. Cette faille étant de plus en plus connue parmi les cybercriminels, elle risque de s'étendre dans un futur proche, tout comme les outils qu'ils mettent en œuvre pour leurs attaques.
- Les parts de marché du navigateur IE ont chuté : s'élevant à 40 % il y a encore quelques années, elles n'atteignent plus que 25 % aujourd'hui.
- Mozilla et Google Chrome sont les navigateurs les plus utilisés en Europe. Internet Explorer est cependant majoritairement utilisé dans des pays comme le Danemark, certaines régions d'Italie, les Pays-Bas, Monaco mais également le Groenland. IE demeure un navigateur largement utilisé par les Européens et des moyens de précaution sont donc nécessaires.
- IE est le navigateur principalement utilisé en Chine, en Angola et au Groenland par exemple.<sup>1</sup>

Le professeur Udo Helmbrecht, [directeur exécutif](#) de l'ENISA, a commenté :

- *« Nous devons accélérer les investissements dans le domaine de la prévention liée à la cybersécurité afin d'être correctement préparés, en équipant les organismes européens avec les ressources adéquates si nous voulons assurer la protection de l'économie et de la société moderne européenne. Aujourd'hui, nous considérons que l'accès à Internet est quelque chose d'acquis, mais même 40 ans après sa naissance et 20 ans de dépendance à la toile cybernétique, de nombreux défis en matière de sécurité sont à relever si nous souhaitons continuer de pouvoir profiter de ses avantages. »*

L'ENISA conseille aux utilisateurs internet de se référer à Microsoft pour toute nouvelle information. Entretemps, la précaution reste de mise pour tous les consommateurs privés. Cette situation mène à tirer des leçons : il est plus coûteux à contrecoup de ne pas investir dès maintenant dans la cybersécurité.

#### Contexte :

**Pour toute demande d'interview, veuillez consulter** Ulf Bergström, Responsable de la communication interne et porte-parole, [ulf.bergstrom@enisa.europa.eu](mailto:ulf.bergstrom@enisa.europa.eu), téléphone portable : + 30 6948 460 143

<sup>1</sup> [http://commons.wikimedia.org/wiki/File:Countries\\_by\\_most\\_used\\_web\\_browser.svg](http://commons.wikimedia.org/wiki/File:Countries_by_most_used_web_browser.svg)



**29/04/2014**

EPR10/15

[www.enisa.europa.eu](http://www.enisa.europa.eu)

*Veillez noter: traduction. La version anglaise est la seule version officielle*

[www.enisa.europa.eu/media/enisa-en-francais/](http://www.enisa.europa.eu/media/enisa-en-francais/)

[www.enisa.europa.eu](http://www.enisa.europa.eu)

L'ENISA est le centre d'expertise pour les questions de sécurité des réseaux et de l'information en Europe

Sécuriser la société de l'information en Europe

L'Agence européenne en charge de la sécurité des réseaux et de l'information

Suivez les affaires de l'ENISA en matière de cybersécurité en Europe sur [Facebook](#), [Twitter](#), [LinkedIn](#), [YouTube](#) & [RSS feeds](#)

