

Les experts annoncent un accord sur les 25 erreurs de programmation les plus dangereuses - et comment les réparer

Cet accord changera la façon dont les organisations achètent les logiciels

Chef de projet : Bob Martin, MITRE

Questions : [top25@sans.org](mailto:top25@sans.org)

(Le 12 janvier 2009) Aujourd'hui à Washington DC, des experts de plus de 30 organisations de cybersécurité américaines et internationales ont conjointement publié le consensus des 25 erreurs de programmation les plus dangereuses qui mènent à des bogues de sécurité et qui permettent le cyber-espionnage et le cyber-crime. Étonnement, la plupart de ces erreurs ne sont pas bien comprises par les programmeurs ; la façon de les éviter est très peu enseignée par les programmes d'informatique ; et leur présence est très peu fréquemment testée par les organisations qui développent des logiciels pour la vente.

L'influence de ces erreurs va très loin. Rien que deux d'entre elles ont déjà mené à des brèches de sécurité dans plus de 1,5 millions de sites web en 2008 - et ces brèches se sont répercutées sur les ordinateurs de ceux qui ont visité ces sites web, transformant leurs ordinateurs en zombies.

Les personnes et organisations qui ont apporté des données substantielles au projet sont listées plus bas. Elles font partie des experts en sécurité les plus respectés et ils viennent des sociétés les plus importantes allant de Symantec et Microsoft à *DH's National Cyber Security Division* et *NSA's Information Assurance Division*, à OWASP et à l'IPA japonaise, jusqu'à l'Université de Californie à l'Université de Davis&Purdue. Le MITRE et l'Institut SANS ont dirigé l'initiative du Top 25 des Erreurs, mais la motivation pour ce projet venait de l'Agence de Sécurité Nationale et le support financier pour les ingénieurs du MITRE venait de la *Division National Cyber Security* du *Department of Homeland Security* américain. L'*Information Assurance Division* de la NSA et la *National Cybersecurity Division* du DHS ont sans équivoque été les meneurs du gouvernement pour travailler à l'amélioration de la sécurité des logiciels achetés par le gouvernement et par les infrastructures nationales les plus importantes.

Ce qui était remarquable dans le projet était la rapidité avec laquelle tous les experts sont tombés d'accord, en dépit de débats éprouvants. « *Il semble y avoir un accord général sur les erreurs de programmation* », explique le directeur du SANS, Mason Brown, « *Maintenant il est temps de les réparer. Premièrement nous devons nous assurer que chaque programmeur sait comment écrire un code sans aucune des erreurs du Top 25, et ensuite nous devons être sûrs que chaque équipe de programmation a les moyens de trouver, réparer, ou éviter ces problèmes et qu'elles ont les outils nécessaires pour vérifier l'infailibilité de leur code aussi bien que des outils automatiques peuvent le faire.* »

Le Bureau du Directeur de l'Intelligence Nationale a exprimé son soutien en disant, « *Nous croyons que l'intégrité du matériel et des logiciels informatiques est un élément important de la cybersécurité. Créer plus de logiciels sûrs est un aspect fondamental de la sécurité du système et du réseau, étant donné que le gouvernement fédéral et les infrastructures nationales les plus importantes dépendent de produits commerciaux pour des opérations d'affaires. Le Top 25 est un composant important d'une initiative de sécurité totale pour notre pays. Nous applaudissons cet effort et encourageons l'utilité de cet outil à travers d'autres branches comme la cyber-éducation.* »

Jusqu'à maintenant, la plupart des informations se concentraient sur les "points faibles" qui résultaient de la programmation d'erreurs. C'est bien utile. Le Top 25, cependant, se concentre sur les erreurs de programmation actuelles, faites par des développeurs qui ont créé les points faibles. Tout aussi important, le site web du Top 25 fournit des informations détaillées et des renseignements sur les mesures d'atténuation. « *Maintenant, avec le Top 25, nous pouvons passer moins de temps à*

*travailler avec la police après que la maison ait été dévalisée et à la place se concentrer sur la mise en place de verrous sur les portes avant que ça n'arrive. »* explique Paul Kurtz, un des auteurs principaux de la *US National Strategy to Secure Cyberspace* et le directeur exécutif du *Software Assurance Forum for Excellence in Code* (SAFECode).