Common Criteria EAL4+ : Microsoft veut rassurer ses clients

Depuis plusieurs années, Microsoft subit les foudres des chercheurs de failles qui ne cessent de mettre en avant les faiblesses des systèmes et logiciels de l'éditeur de Redmond.

Pour pallier le déficit de confiance inhérent aux vulnérabilités découvertes au sein de ses produits, Microsoft s'est engagé, il y a trois ans, dans un programme baptisé « *Security Development Lifecycle* » (SDL), dont l'objectif à moyen terme est d'améliorer la qualité et la sécurité de ses développements. L'obtention des certifications Common Criteria EAL4+ pour Windows Server 2003, Windows XP SP2, Exchange Server 2003 et ISA Server 2004 découle de cette politique. **Que sont les Critères Communs ?** Les critères communs sont une série de standards approuvés par l'ISO qui permettent, en fonction de critères spécifiques, de procéder à l'évaluation du niveau de sécurité d'un logiciel. L'évaluation est graduée sur une échelle de 1 à 7. Le niveau 7 possède les critères les plus rigoureux. EAL4 est le niveau maximum qu'un logiciel puisse obtenir afin qu'il soit reconnu par les 22 pays signataires des Critères Communs (France, USA, Canada, Australie, Allemagne, Italie, Espagne, Inde, Israël, Suède…). Le signe '+' signifie que des tests de vulnérabilité ont également été menés sur l'application afin d'en garantir la sécurité. **Microsoft veut rassurer ses clients** Microsoft a annoncé aujourd'hui que Windows Server 2003 SP1 (édition Standard, Enterprise et Datacenter), Windows 2003 Certificate Server, Windows XP PRO SP2 (et '*embedded*' – embarqué), ainsi qu'Exchange Serveur 2003 et ISA Server 2004 répondent désormais aux Critères Communs EAL4+. L'évaluation de SQL Server est en cours. Des codes sources des logiciels testés ont été transmis à l'organisme en charge de la certification afin d'auditer les solutions en profondeur et parer à tous les scénarios. Cette certification, délivrée par un laboratoire indépendant, permet aux utilisateurs de mettre en ?uvre une sécurité de bout en bout en disposant des consignes de paramétrage utilisées lors de la certification. Il est donc désormais possible de définir un profil « sécurité » à mettre en ?uvre dans un contexte de conformité EAL4+. EAL4+ apporte un niveau d'assurance aux clients, mais est parfois nécessaire dans certains pays pour répondre aux appels d'offres dans des domaines d'activité sensibles comme le militaire ou le gouvernemental. ISA et Exchange ont été évalués en Allemagne tandis que Windows l'a été aux Etats-Unis. Le processus de certification EAL4+ pour Windows XP Windows 2003 a duré prés de deux ans et demi. **Aurélien Cabezon** pour **Vulnerabilite.com.**