Failles critiques dans les produits ZoneLabs et Computer Associates

Ca fait mauvais effet. Les logiciels anti-virus des éditeurs ZoneLabs et Computer Associates sont impactés par des failles qualifiées de « critiques ».

Chez Computer Associates, la faille critique découverte par Alex Wheeler pourrait être exploitée par un attaquant distant ou un ver/virus afin de compromettre un système vulnérable. Selon FrSIRT, le problème est issu d'une erreur de type *heap overflow* présente dans la librairie Vet (VetE.dll) qui ne gère pas correctement certaines macro-commandes VBA contenant des entêtes malformées, ce qui pourrait être exploité afin d'exécuter des commandes arbitraires distantes en envoyant, vers un antivirus vulnérable, un document Microsoft Office spécialement conçu. eTrust Antivirus 6.0, 7.0, 7.1 pour Windows, Linux, Note/Exchange, Solaris, eTrust EZ Antivirus 7.x, eTrust Intrusion Detection 1.4.1.13, 2.0, 3.0, eTrust Secure Content Manager 1.x, InoculateIT 6.0 et BrightStor ARCserve Backup (BAB) r11.1 sont impactés. Computer Associates a mis en ligne un correctif de sécurité inclus avec les nouvelles signatures Vet. Comme les logiciels anti-viraux de ZoneLabs intégrent le moteur antiviral Vet de Computer Associates, ses produits anti-virus (et seulement ceux-ci) sont aussi impactés. Chez ZoneLabs, ce n'est pas la première fois qu'un produit présente un « trou » important. Un coup dur pour l'image de l'éditeur du célèbre ZoneAlarm. Découverte également par Alex Wheeler et communiquée par le site de veille FrSIRT, la vulnérabilité pourrait être exploitée par un attaquant distant ou un ver/virus afin de compromettre un système vulnérable. Selon le site spécialisé, le problème est la conséquence d'une erreur de type *heap overflow* présente dans la librairie Vet (VetE.dll) qui ne gère pas correctement certaines macros VBA contenant des entêtes malformées. La faille pourrait être exploitée afin d'exécuter des commandes arbitraires distantes en envoyant, vers un antivirus vulnérable, un fichier malicieux contenant une macro VBA spécialement conçue. ZoneAlarm Antivirus (toutes versions) et ZoneAlarm Security Suite (toutes versions) sont impactées. Pour l'heure, il n'existe pas encore de 'patch' ni de remède « officiel ».