

Failles critiques chez Symantec, un comble !

Sur

Norton Internet Security, la méthode '*LaunchURL*' du composant ActiveX de la classe '*WrapNISUM*' (WrapUM.dll) permet d'exécuter du code arbitraire à partir d'un poste distant. Cette faille peut être exploitée afin d'inciter l'utilisateur à afficher un document HTML corrompu, soit en visitant un site Web, soit sur un email au format html. Quant à **Norton AntiSpam 2004**, une erreur binaire dans la classe '*SymSpamHelper*' du composant ActiveX peut être exploitée et entraîner une surcharge de la mémoire (*buffer overflow*) en fournissant à la méthode '*LaunchCustomRuleWizard*' un paramètre excessivement long. Les 'patches' de corrections sont disponibles sur la plateforme de mise à jour de Symantec. Ces failles sont jugées d'autant plus critiques, nonobstant le risque qu'elles représentent si elles sont exploitées, que les produits Norton de Symantec sont théoriquement destinés à protéger leurs utilisateurs...