Faille dans Sendmail (2): pourquoi c’est sérieux…

La cellule X-Force d’Internet Security Systems (ISS) est à l’origine de la découverte. La vulnérabilité de type « race condition » affecte les versions les plus récentes de Sendmail. Le défaut de sécurité est localisé dans une fonction appelée lors du traitement d’un message électronique.

L’exploitation de la faille nécessite l’envoi d’emails piégés en suivant un « timing » bien particulier. En cas de réussite, il serait possible d’exécuter des commandes arbitraires avec les droits alloués au processus Sendmail. La confidentialité, l’intégrité et la disponibilité des emails seraient alors remises en question. Pour l’heure , Sendmail annonce sur son site Internet qu’aucun exploit profitant de cette nouvelle faiblesse ne circule sur la Toile? Mais pour combien de temps ? Quoi qu’il en soit, les équipes de Sendmail ont toujours fait preuve d’une remarquable réactivité ce qui permet aux utilisateurs et clients de l’éditeur de diminuer la fenêtre d’exposition aux risques. Un correctif et une nouvelle version de Sendmail (8.13.6) sont d’ores et déjà disponibles sur le site de l’éditeur. Ce n’est pas la première fois que l’image de Sendmail se voit entachée d’une vulnérabilité critique. En 2003, deux failles (dont l’une fut également découverte par ISS) ouvraient aux pirates la possibilité d’exécuter du code à distance. Il y a plus de 10 ans, c’est une vulnérabilité dans Sendmail qui avait permis à l’un des plus médiatiques pirates américains, Kevin Mitnick, de s’introduire au c?ur de réseaux d’opérateurs Internet.