

# [Faille de sécurité 'critique' sur des jeux-vidéos en ligne](#)

Plus discrètes, les failles dans les jeux-vidéos sont certes moins nombreuses que dans les applications mais tout aussi dangereuses. Une vulnérabilité critique a ainsi été identifiée dans « Unreal Engine », le gestionnaire de réseau utilisé par de nombreux jeux-vidéos jouables en ligne.

Qualifiée de « hautement critique » par Secunia, elle touche 15 jeux (voir liste en encadré), quelque soit le système d'exploitation utilisé. La faille exploitée permet à une personne malveillante de prendre le contrôle à distance d'un serveur afin de l'utiliser comme passerelle pour attaquer d'autres machines. « Unreal Engine » permet d'identifier si un serveur de jeu en réseau est bien dédié à ce logiciel. Une personne malintentionnée pourrait l'exploiter pour créer un dépassement de mémoire tampon (buffer overflow). Le programme accède alors à des zones mémoire qui ne lui sont pas destinées. Une situation qui peut ensuite être exploitée pour exécuter du code à distance sur la machine cible, afin d'en prendre le contrôle. Un premier patch est disponible, notamment pour le jeu Unreal à l'adresse: <http://www.unrealtournament.com/ut2004/downloads.php> **Liste des jeux vulnérables**

DeusEx (build 1.112fm and prior) Devastation (build 390 and prior) Mobile Forces (build 20000 and prior) Nerf Arena Blast (build 1.2 and prior) Postal 2 (build 1337 and prior) Rune (build 107 and prior) Tactical Ops (build 3.4.0 and prior) TNN Pro Hunter Unreal 1 (build 226f and prior) Unreal II XMP (build 7710 and prior) Unreal Tournament (build 451b and prior) Unreal Tournament 2003 (build 2225 and prior) Unreal Tournament 2004 (prior to build 3236) Wheel of Time (build 333b and prior) X-com Enforcer