PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 4 - numero 586 di giovedì 27 giugno 2002

Individuata falla nel software OpenSSH

A causa di questa vulnerabilita' un aggressore riuscirebbe ad eseguire da remoto un codice a sua scelta.

E' stata individuata in questi giorni una falla nell'ultima versione del software open source OpenSSH, che crittografa tutto il traffico di rete (comprese le passwords) per eliminare possibili intercettazioni delle comunicazioni.

In base a quanto pubblicato su LinuxSecurity.com da Theo de Raadt, uno degli sviluppatori del team OpenBSD, e riportato da un quotidiano esperto di sicurezza informatica, a causa di questa vulnerabilità un aggressore potrebbe eseguire da remoto un codice a sua scelta.

Al momento non è ancora disponibile una patch, ma fortunatamente l'ultima versione del software OpenSSH 3.3p è stata rilasciata pochi giorni fa ed è quindi poco probabile che sia già stata installata con particolari valenze dal punto di vista della sicurezza.

Per limitare i rischi connessi all'utilizzo di OpenSSH 3.3p è, però, possibile attivare la funzione "Privilege Separation", dal file di configurazione "/etc/ssh/sshd_config".
Secondo Raadt, infatti, se l'opzione "Privilege Separation" è attiva di default la vulnerabilità non può essere sfruttata da remoto.
