PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 4 - numero 640 di venerdì 11 ottobre 2002

Un codice malevolo in alcune copie di Sendmail

Server a rischio. L'allarme e' stato lanciato dal CERT.

In alcune copie di Sendmail, mail server open-source molto diffuso, è stato inserito da un "intruso" un codice malevolo, un Trojan horse, capace di mettere in grave pericolo la sicurezza del server sul quale il programma viene compilato.

La notizia è stata diffusa dal CERT, che in un bollettino di sicurezza, ha fornito agli amministratori di sistema le indicazioni per verificare la sicurezza del software.

Il problema è stato riscontrato nella versione 8.12.6 di Sendmail scaricabile dal server FTP ftp.sendmail.org tra il 28 settembre e il 6 ottobre 2002; il Trojan horse era contenuto nei file sendmail.8.12.6.tar.Z sendmail.8.12.6.tar.gz.
In ogni caso il CERT raccomanda anche a coloro che in quel periodo hanno utilizzato copie distribuite attraverso i server HTTP di seguire, per precauzione, la procedura indicata nel bollettino ("Solution").

Il Trojan horse è in grado di creare una backdoor sulla porta 6667/tcp, attraverso la quale un intruso potrebbe ottenere l'accesso remoto al server con gli stessi privilegi di chi ha compilato il programma.
