Múltiplas Vulnerabilidades em diversas aplicações de terceiros. Não negligencie seu servidor!

Autoria de Redação FUG-BR

13/08/2006

Última Atualização 14/08/2006

Sistemas BSD são conhecidos em geral por sua estabilidade, performance e segurança. Mas é importante lembrar que no último quesito, não adianta apenas ter um sistema top no que tange a segurança, e simplesmente ignorar problemas nas aplicações utilizadas nesse sistema. Não estamos falando de BSD, Linux, Windows ou Mac em especial. Isso vale para todo e qualquer sistema. A diferença é que alguns são desenvolvidos de forma mais elegante e maior respeito ao usuário. No FreeBSD você tem por exemplo uma incrível ferramenta chamada portaudit que através de um database de vulnerabilidades centralizado, permite que você faça a auditoria de segurança de suas aplicações localmente instaladas. Tem o portupgrade para auxiliar e facilitar a atualização de ports. Tem portsnap para atualizar suas definições locais de ports. O portaudit, portupgrade e portsnap já foram documentados dezenas de vezes ao longo dos artigos aqui na FUG. Mas você está usando-os? Ou pelo menos, acompanha o RSS e/ou o site do VuXML ? E olha que é muito simples, aqui no site da FUG por exemplo , no menu esquerdo tem um submenu chamado Alertas em Ports bem na cara, para chamar sua atenção.

Pois bem, nos últimos 5 dias, 10 problemas de segurança em aplicações de terceiros foram documentados, e é muito provável que você use algumas dessas aplicações. Só hoje foram 5! Você está alerta? Aplicações populares como MySQL, PostgreSQL, Squirrel Mail, Drupal e Clam-AV estão na lista. Ainda que você tenha rotinas chflags e securelevel alto, que tenha centenas de Políticas POSIX.1e em dezenas de camadas de abstração MAC, ou que não use os maiores recursos de segurança nativa de sistemas BSD: não há desculpa, aplicações de terceiros, não podem ser negligenciadas.

Então mãos à obra, acesse <http://www.vuxml.org/freebsd/> e seja pro-ativo. Esse fato não deveria ter se tornado uma notícia, deveria ser algo óbvio e intuitivo, mas devido a algumas conversas que eu - um dos membros do time www - tive no IRC com alguns sysadmins BSD e Linux, fiquei desconfortável ao notar que a maioria não deu atenção a quantidade de problemas publicados, especialmente hoje. Então fica o alerta para chamar atenção!