Obtendo chave de criptografia de disco c/ memory dump após Cold Reboot: Pq FreeBSD não é vulnerável?

Autoria de Redação FUG-BR.
24/02/2008
Última Atualização 24/02/2008

Existem certas curiosidades que só acontecem mesmo quando a liberdade de uma comunidade não é menor que sua dedicação. Algumas vezes por exemplo, dentro de uma thread de discussão em uma lista, ou em um fórum, temos informações mais completas e precisas vidas do leitor, do que de fato do autor.

Não que seja exatamente o caso, mas desta feita, temos que citar uma notícia de propósito geral, sobre segurança em TI, publicada no site BR-Linux, sobre a possibilidade de exploração com sucesso de acesso a dados em partições e devices criptografados de disco, possível com um simples memory dump após um Cold Reboot, publicado nesse endereço.

Ao longo da notícia temos três posts detalhados que ilustram porque, o FreeBSD, em suas duas principais implementações de criptografia de disco, não está vulnerável a esse tipo de exploração física da estação. A explicação é clara, razoável, e convincente. Porém, quando consultado por nossa equipe sobre essas informações, o desenvolvedor PJD informou que a informação está correta, mas que vai publicar nessa semana que se inicia testes aplicando essa metodologia para ilustrar como na prática o FreeBSD não está vulnerável ao problema.

Como trata-se de uma explicação técnica dentro de um contexto, ao invés de reproduzirmos os posts do usuário grab, é mais indicado que você acesse e leia o conteúdo.