

A resposta do Debian

Matéria do [SecurityFocus](#) de 03/12/2003

As coisas ficaram muito agitadas no mundo Linux recentemente, quando a distribuição Linux Debian anunciou que um cracker invadiu quatro máquinas do projeto debian.org, alcançou privilégios de root, e instalou rootkits em muitos servidores.

O método? O cracker usou um software de keylog para pegar a senha de um usuário autorizado e acessar um dos servidores em 19 de Novembro de 2003, então logou e se beneficiou de uma vulnerabilidade no Kernel do Linux para se tornar root. Depois disso, pouco tempo foi necessário para as outras máquinas do projeto também estarem comprometidas. Maiores detalhes sobre o exploit estão disponíveis em vários locais, incluindo o Linux Today e wiggy.net.

Vamos direto à pergunta que muitos leitores provavelmente estão se fazendo: Se eu uso Linux, devo me preocupar?

Bem, sim e não. A vulnerabilidade usada para obter os privilégios afeta todas as versões do kernel do Linux antes da 2.4.23 (ou 2.5.69 se você está rodando essa série do kernel, ou ainda 2.6.0-test6 se você está usando a mais nova versão). E isso inclui todas as distribuições, seja Debian, Red Hat, Mandrake, Slackware, e SUSE[1]. De qualquer forma, para poder explorar a vulnerabilidade, o cracker, primeiro, deve ter uma conta local na máquina, com acesso ao shell. Em outras palavras, os malfeitores não podem forçar a entrada numa máquina Linux até que eles tenham um modo acessar como um usuário dessa máquina. A resposta curta: As chances são um pouco remotas, mas você deve continuar fazendo os patches(correções) nos seus sistemas e fazer o upgrade para a última versão do kernel tão breve quanto for conveniente. Um sistema comprometido não é uma coisa legal.

Agora, num quadro mais abrangente. O time do Debian é elogiado pelo modo como eles trataram esse incidente: rapidamente, abertamente e honestamente. A falha foi descoberta em 20 de novembro; foi publicamente anunciada em 21 de novembro, um pouco mais que 12 horas depois. Muitas companhias e organizações tentam ofuscar e esconder quando eles são vítimas de brechas de segurança, e isso não beneficia ninguém. O Debian leva a sério o código aberto e a liberdade do software livre - muitas vezes mais seriamente que algumas outras distribuições do Linux- e essa filosofia foi demonstrada publicamente nessas últimas semanas. Parabéns Debian.

Mais parabéns devem ser dados a várias organizações e companhias responsáveis por muitas das mais populares distribuições Linux. Em muitos casos, essas companhias são competidores, mas eles trabalham todos juntos para alisar, corrigir, e publicar correções para o problema. Esse é um grande exemplo de comportamento cooperativo trabalhando no benefício de todos, incluindo as companhias e seus clientes.

Não é nenhuma surpresa que o problema tenha começado no elo mais fraco, os usuários que acessam o sistema. Não estou apontando o dedo para ninguém em particular que teve um keylogger instalado no seu sistema, até mesmo porque não tenho detalhes de como isso aconteceu. Porém, novamente os mestres em segurança precebem que pequenos problemas com usuários finais podem ser tornar enormes problemas para toda uma organização e sua infraestrutura de TI.

Uma vez que alguém toma uma máquina, certas tarefas são inevitáveis. Mais uma vez, o time do Debian fez exatamente o que os leitores do SecurityFocus também fariam: copiar os discos para propósitos judiciais, setivar todas as contas, senhas e chaves ssh nas máquinas e requisitar que todos os usuários mudem suas senhas, e então limpar a máquina e reinstalar do zero. Em detalhamento público dos passos, o Debian fez um serviço aos novatos no campo de segurança, e deu a eles um exemplo de reações necessárias em ataque severo.

Na realidade, o Debian usou o que os educadores gostam de chamar de "teachable moment"(ao pé da letra, momento de educação).Foram feitas recomendações aos usuários e desenvolvedores para usarem o chkrootkit, um programa que checa o sistema por assinaturas de rootkits, como o que foi instalado nos servidores do Debian. Na realidade, uma lista completa de tarefas para cada desenvolvedor Debian que suspeite de comprometimento foi publicada, e ela oferece excelentes avisos numa linguagem bem clara.

Usuários do debian.org vão precisar mudar suas senhas, não apenas nas quatro máquinas Debian, mas em todos os computadores que eles tenham acessado e que requerem senha. Isto, naturalmente, deve lembrar a todos usar senhas diferentes para cada máquina que você acessa. Sim, eu sei que isso é completamente doloroso, mas agora deve ser completamente óbvio o porque isso é necessário.

Há mais algumas lições dolorosas a serem aprendidas a partir desse incidente. Uma notícia do Debian contém o seguinte parágrafo:

Embora esse bug no kernel tenha sido descoberto em setembro por Andrew Morton e corrigido num recente pre-release do Kernel desde outubro, não foi considerada uma implicação severa à segurança. Então nenhum alerta de segurança foi publicado por nenhum distribuidor. De qualquer forma, depois que foi descoberto que isso podia ser usado como uma falha de segurança o projeto "Common Vulnerabilities and Exposures" emitiu o CAN-2003-0961 para esse problema. Isso foi corrigido no Linux 2.4.23 que foi lançado no último fim de semana no Debian advisory DSA 403.

Claramente o julgamento da severidade não tinha base, e como resultado, o Debian pagou o preço. Espero que os mantenedores do kernel aprendam com a lição do Debian, e no futuro trabalhem duro para atualizar o kernel quando necessário.

Quando coisas ruins acontecem a bons sistemas operacionais, é importante corrigir os problemas, aprender com eles e ir em frente. Os problemas que o Debian sofreu nas últimas semanas provarão finalmente ser uma coisa boa para a comunidade Linux, e para os profissionais em segurança também. Espero que o Debian nunca veja outro problema de segurança como esse, mas se acontecer, eu creio que será trabalhado de forma profissional e produtiva como dessa vez.

[1]O autor não colocou mas a distribuição brasileira, Conectiva, também é afetada.

Notícia retirada de: <http://www.securityfocus.com/columnists/202>

Tradução: Rafael Ferreira Silva - <http://www.webphp.com.br>