Dicas de [In]segrança

OpenSSL

O *OpenSSL* é uma biblioteca que implementa os protocolos *Secure Sockets Layer* (SSL v2/v3) e *Transport Layer Security* (TLS v1), bem como um mecanismo de criptografia forte de uso geral.

Colin Percival descobriu um ataque de sincronismo de cache que permitiria a um usuário local malicioso descobrir algumas porções das chaves criptográficas em uso. O projeto "Common Vulnerabilities and Exposures" (cve.mitre.org) deu a essa falha o código CAN-2005-0109.

A biblioteca SSL foi "remendada" para incluir um novo *mod_exp* com tamanho fixo de janela. Esse novo *mod_exp* seria usado como padrão para as operações em RSA, DAS e DH. Espera-se com isso mitigar os ataques de sincronismo de cache e assemelhados.

Uma falha foi encontrada na forma como o script *der_chop* cria arquivos temporários. É possível que um usuário local sem nada melhor para fazer além de sacanear quem precisa trabalhar possa forçar o der_chop a gravar por cima dos arquivos de outrem (CAN-2004-0975). Depois disso, o script der_chop foi tornado obsoleto e retirado das versões mais recentes do OpenSSL. ■

Referência no Mandriva: MDKSA-2005:096

Referência no Red Hat: RHSA-2005:476-08

ImageMagick

O *ImageMagick(TM)* é uma popular ferramenta de visualização e manipulação de imagens para o *X Window System* que reconhece um enorme número de formatos de imagem.

Um estouro de buffer na pilha de dados (*heap*) do processo foi encontrado nas rotinas de manipulação de arquivos no formato PNM. Um agressor poderia facilmente executar código arbitrário na máquina da vítima se puder persuadi-la a abrir um arquivo PNM especialmente criado. O projeto "Common Vulnerabilities and Exposures" (cve.mitre.org) deu a essa falha o código CAN-2005-1275.

Postura das principais distribuições Linux quanto à segurança

Distribuição	Referência de Segurança	Comentários
Conectiva	Info: http://distro2.conectiva.com.br/ Lista: seguranca-admin@distro.conectiva.com.br e http://distro2.conectiva.com.br/lista/ Referência: CLSA-... [1]	Possui uma página específica; não há link para ela na página principal. Os alertas são sobre segurança, mas distribuídos através de emails assinados com a chave PGP da empresa para assegurar sua autenticidade. Contém também links para os pacotes atualizados e para fontes de referência sobre o problema sendo corrigido.
Debian	Info: http://www.debian.org/security/ Lista: http://lists.debian.org/debian-security-announce/ Referência: DSA-... [1]	Alertas de segurança recentes são colocados na homepage e distribuídos como arquivos HTML com links para os patches. O anúncio também contém uma referência à lista de discussão.
Gentoo	Info: http://www.gentoo.org/security/en/gsla/index.html Fórum: http://forums.gentoo.org/ Lista: http://www.gentoo.org/main/en/lists.xml Referência: GLSA: ... [1]	Os alertas de segurança são listados no site de segurança da distribuição, com link na homepage. São distribuídos como páginas HTML e mostram os comandos necessários para baixar versões corrigidas dos softwares afetados.
Mandrake	Info: http://www.mandrakesecure.net Lista: http://www.mandrakesecure.net/en/mlist.php Referência: MDKSA-... [1]	A MandrakeSoft tem seu próprio site sobre segurança. Entre outras coisas, inclui alertas e referência a listas de discussão. Os alertas são arquivos HTML, mas não há links para os patches.
Red Hat	Info: http://www.redhat.com/errata/ Lista: http://www.redhat.com/mailing-lists/ Referência: RHSA-... [1]	A Red Hat classifica os alertas de segurança como "Erratas". Problemas com cada versão do Red Hat Linux são agrupados. Os alertas são distribuídos na forma de páginas HTML com links para os patches.
Slackware	Info: http://www.slackware.com/security/ Lista: http://www.slackware.com/lists/ (slackware-security) Referência: [slackware-security] ... [1]	A página principal contém links para os arquivos da lista de discussão sobre segurança. Nenhuma informação adicional sobre segurança no Slackware está disponível.
SUSE	Info: http://www.novell.com/linux/security/ Lista: http://www.novell.com/linux/download/updates/ Referência: suse-security-announce Referência: SUSE-SA ... [1]	Após mudanças no site, não há mais um link para a página sobre segurança, que contém informações sobre a lista de discussão e os alertas. Patches de segurança para cada versão do SUSE LINUX são mostrados em vermelho na página de atualizações. Uma curta descrição da vulnerabilidade corrigida pelo patch é fornecida.

[1] *Todas as distribuições indicam, no assunto da mensagem, que o tema é segurança.*

Todos os usuários do ImageMagick devem atualizar o programa, que contém um patch trazido das versões posteriores e não está vulnerável a essa falha. ■

Referência no Gentoo: GLSA 200505-16 / ImageMagick

Referência no Red Hat: RHSA-2005:413-04

❒ gFTP

O *gFTP* é um cliente gráfico e multitarefa de FTP. Uma falha de travessia de diretórios foi encontrada no gFTP. Se um usuário for levado a baixar um arquivo de um servidor de FTP imundo, é possível sobrescrever arquivos da própria vítima. O projeto "Common Vulnerabilities and Exposures" (cve.mitre.org) deu a essa falha o código CAN-2005-0372.

Todos os usuários do gftp devem atualizar o programa o mais rápido possível. ■

Referência no Red Hat:RHSA-2005:410-07

❒ gEdit

O *gEdit* é um pequeno e muito versátil editor de textos escrito especificamente para o ambiente Gnome.

Uma vulnerabilidade de formatação em cadeias de caracteres no nome do arquivo foi encontrada no gEdit. É possível que um agressor crie um arquivo com um nome tal que, quando aberto, execute instruções arbitrárias na máquina da vítima. Embora seja incomum um usuário abrir um arquivo que contenha um nome com código embutido (e, portanto, pra lá de estranho) é fácil engabelá-lo se o arquivo vier por email, por exemplo – e, como todos sabem, os usuários têm compulsão de sair clicando em tudo o que vem por email. O projeto "Common Vulnerabilities and Exposures" (cve.mitre.org) deu a essa falha o código CAN-2005-1686.

É fortemente recomendado que todos os usuários do gEdit atualizem suas cópias desse programa para a última versão estável. ■

Referência no Gentoo:GLSA 200506-09 / gedit

Referência no Red Hat:RHSA-2005:499-05

❒ Mozilla

O *Mozilla* é um navegador de Internet de código aberto que contém, além disso, um poderoso cliente de email e notícias, um cliente de bate-papo IRC e um editor de páginas HTML.

Muitas brechas foram encontradas na maneira como o Mozilla executa código *JavaScript*. O JavaScript executado a partir de uma página deveria rodar com níveis restritos de acesso, evitando assim ações potencialmente perigosas. O Mozilla, mais uma vez, colabora com os meliantes permitindo que páginas criminosas executem código JavaScript com privilégios elevados, garantindo acesso a dados e funções protegidos. O projeto "Common Vulnerabilities and Exposures" (cve.mitre.org) deu a essa falha os códigos CAN-2005-1476, CAN-2005-1477, CAN-2005-1531 e CAN-2005-1532.

Todos os usuários do Mozilla são aconselhados a atualizar o programa para a versão 1.7.8. ■

Referência no Gentoo:GLSA 200505-11 / mozilla

Referência no Red Hat:RHSA-2005:434-10; RHSA-2005:435-14

Referência no Slackware:SSA:2005-135-01

Referência no SuSE:SUSE-SA:2005:030

❒ FreeRadius

O *FreeRADIUS* é um popular servidor de autenticação pelo protocolo RADIUS de código aberto.

Primoz Bratanic descobriu que a função *sql_escape_func* do FreeRADIUS pode estar vulnerável a um estouro de buffer (BID 13541). Como se não bastasse, o FreeRADIUS falha ao "higienizar" os dados informados pelo usuário antes de inseri-los em uma consulta SQL. Resultado: o programa vergonhosamente cai de joelhos frente a um ataque por injeção de comandos SQL – algo bem amador (BID 13540).

Ao inserir dados cuidadosamente selecionados, um usuário com intenções escusas pode injetar (e executar) comandos SQL arbitrários ou causar um estouro

de buffer. No primeiro caso, o agressor pode obter ou mesmo modificar dados importantes; no segundo caso, ele pode travar o servidor e causar um ataque de negação de serviço.

Infelizmente, não há maneira de contornar o problema. Todos os usuários do FreeRADIUS devem atualizar o programa para a versão mais atual. ■

Referência no Gentoo: GLSA 200505-13 / freeradius

Referência no SuSE: SUSE-SR:2005:014

Mailutils

O *GNU Mailutils* é um conjunto de utilitários para leitura e manipulação de mensagens de correio eletrônico, o popular e-mail, incluindo um servidor IMAP4 (chamado *imap4d*) e um cliente de email (o comando *mail*).

Um certo *infamous41d* descobriu inúmeras vulnerabilidades no GNU Mailutils. Por exemplo, o imap4d não implementa corretamente a exibição correta de marcas de comando (CAN-2005-1523), falha ao validar a seqüência de alcance do comando *FETCH* (do protocolo IMAP – CAN-2005-1522) e contém um estouro de inteiros na rotina *fetch_io* (CAN-2005-1521). O comando mail contém um estouro de buffer na função *header_get_field_name( )* (CAN-2005-1520).

Um agressor remoto poderia explorar as falhas de formato de cadeia de caracteres e de estouro de inteiros no imap4d para executar código arbitrário como o usuário que executa o imap4d – normalmente o *root* (aiaiai...).

Ao enviar uma mensagem de email especialmente manipulada, um agressor remoto poderia também explorar o estouro de buffer no comando mail para executar código arbitrário com os direitos do usuário que o está usando. Agora pense: o usuário comum costuma usar clientes mais poderosos como *Mutt, Evolution, Pine, Kmail* e cia. Quem é que costuma usar o comando mail, então? Isso mesmo: o *root*.

Finalmente, um agressor remoto poderia provocar uma negação de serviço com o envio de comandos FETCH maliciosos para um servidor imap4d vulnerável, causando exaustão de recursos.

Recomenda-se que todos os usuários do GNU Mailutils atualizem o programa para a última versão. ■

Referência no Debian:DSA-732-1

Referência no Gentoo: GLSA 200505-20 / mailutils; GLSA 200506-02 / mailutils

Gaim

O *Gaim* é um programa de mensagens instantâneas que pode trabalhar com uma grande quantidade de protocolos, entre eles os populares *MSN, ICQ, Jabber, SILC* e o *Yahoo! Messenger*.

Stu Tomlinson descobriu que o Gaim é vulnerável a um estouro de buffer na pilha quando recebe mensagens de certos protocolos como o Jabber e o SILC. O agressor cria mensagens que possuam URLs muito grandes (CAN-2005-1261). Mas os problemas não para por aí. Siebe Tolsma descobriu que o Gaim também pode ser tirado do ar remotamente através de mensagens no protocolo MSN (CAN-2005-1262).

O estouro de buffer pode ser ativado remotamente por meio de uma URL muito longa, potencialmente levando à execução de código abominável. Já uma mensagem SLP com o corpo vazio (i.e. só o datagrama sem dado algum) poderia causar uma negação de serviço – um verdadeiro tiro no peito.

Já Jacopo Ottaviani descobriu uma vulnerabilidade no código de transferência de arquivos usado pelo protocolo do Yahoo! Messenger. A falha se apresenta quando o nome do arquivo contém caracteres especiais não ASCII (CAN-2005-1269). Hugo de Bokkenrijder descobriu uma vulnerabilidade em mensagens malformadas pelo protocolo MSN (CAN-2005-1934). Ambas as falhas fazem o Gaim se enforcar, causando uma negação de serviço.

Não há maneira de se contornar o problema. Todos os usuários do Gaim devem atualizar o programa para a versão mais nova. ■

Referência no Gentoo: GLSA 200505-09 / gaim; GLSA 200506-11 / gaim

Referência no Slackware: SSA:2005-133-01 e também SSA:2005-162-01

Referência no SuSE: SUSE-SR:2005:015

gzip

O *gzip* é um sistema de compactação e empacotamento de arquivos muito usado. Inúmeras vulnerabilidades foram descobertas neste programa.

O utilitário *zgrep* das versões anteriores à 1.3.5 do gzip não faz a faxina prévia nos argumentos informados pelo usuário, o que permite que vagabundos sem noção executem código arbitrário por meio de nomes de arquivos injetados em um script *sed*. (CAN-2005-0758)

Uma condição de disputa (*race condition*) no gzip 1.2.4, 1.3.3 e mais antigos durante a descompactação permite que usuários locais modifiquem as permissões de arquivos arbitrários pela técnica do "ataque por *hardlinks*". O gzip só altera as permissões de um arquivo quando a descompactação está completa. (CAN-2005-0988)

Uma falha de travessia de diretórios via `gunzip -N` no gzip versões 1.2.4 até 1.3.5 permite que agressores remotos escrevam em diretórios arbitrários. A técnica usada é a manjadíssima "um diretório acima", em que os caracteres ".." (ponto ponto) são inseridos no nome original do arquivo dentro do pacote compactado, fazendo referência a um diretório "pai" que deveria estar fora do alcance do atacante. (CAN-2005-1228)

Os pacotes atualizados usados pelas principais distribuições estão "remendados" para incluir correções. ■

Referência no Gentoo:GLSA 200505-05 / gzip

Referência no Mandriva:MDKSA-2005:092

Referência no Red Hat:RHSA-2005:357-19