Dicas de [In]segurança

MySQL

O MySQL é um banco de dados multiusuário e multiprocesso. Foram divulgadas algumas falhas de segurança que afetam o pacote mysql-server. Oleksandr Byelkin descobriu que a declaração "ALTER TABLE ... RENAME" verificava as permissões de criação e inserção de dados (CREATE/INSERT) da tabela antiga e não da nova. O projeto "Common Vulnerabilities and Exposures" (cve.mitre.org) deu a essa falha o código CAN-2004-0835.

Lukasz Wojtow descobriu um estouro de buffer (*buffer overrun*) na função *mysql_real_connect*. Para explorar essa falha o atacante deve forçar o uso de um servidor DNS "envenenado", com registros maliciosos (CAN-2004-0836).

Dean Ellis descobriu que, se vários processos modificarem (declaração ALTER) a mesma tabela MARGE (ou mesmo tabelas diferentes) para mudar o parâmetro UNION, o servidor poderá travar (CAN-2004-0837).

Sergei Golubchik descobriu que, se um usuário possuir um nome com o caracter sublinhado ("_") e tiver algum privilégio de acesso, pode atribuir privilégios a outros usuários de bancos de dados com nomes semelhantes (CAN-2004-0957).

Há ainda um grande número de pequenas falhas, incluindo alguns problemas potenciais de segurança associados à manipulação descuidada de arquivos temporários. O projeto "Common Vulnerabilities and Exposures" (cve.mitre.org) deu a essas falhas os códigos CAN-2004-0381, CAN-2004-0388 e CAN-2004-0457. ■

Referência no Gentoo: GLSA 200410-22 / MySQL
Referência no Mandrake: MDKSA-2004:119
Referência no Red Hat: RHSA-2004:569-16

CUPS

O *Common UNIX Printing System* (CUPS) é um sistema de impressão para Unix. Durante uma auditoria no código fonte, Chris Evans descobriu um número razoável de falhas envolvendo estouro de buffers de inteiros que afetam o programa xpdf. O CUPS contém uma cópia do xpdf, que é usada para interpretar arquivos em PDF para impressão e, portanto, é afetado por esses *bugs*. Um invasor que consiga enviar um PDF maliciosamente preparado para impressão pode causar o travamento do CUPS ou até mesmo executar código arbitrário. O projeto "Common Vulnerabilities and Exposures" (cve.mitre.org) deu a essa falha o código CAN-2004-0888.

Quando configurado para imprimir em uma impressora remota via Samba, o CUPS pode se autenticar nela utilizando um usuário e senha.

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 à 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.suse.de/uk/private/support/security/* Lista: *http://www.suse.de/uk/private/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.

Por padrão, o nome do usuário e sua senha são gravados pelo Samba no arquivo de registro de erros (log). Um usuário local com permissão para ler o registro tem total acesso aos logins e senhas de todos os usuários que imprimiram algo. O projeto "Common Vulnerabilities and Exposures" (cve.mitre.org) deu a essa falha o código CAN-2004-0923.

Os pacotes atualizados também incluem correções que evitam que alguns dos arquivos de configuração do CUPS sejam substituídos. ■

Referência no Debian: DSA-581-1 xpdf
Referência no Mandrake: MDKSA-2004:116
Referência no Red Hat: RHSA-2004:543-15
Referência no SuSE: SUSE-SA:2004:039

libtiff

A libtiff é uma biblioteca usada por visualizadores de imagem – o que também inclui os navegadores de Internet – para manipular e exibir imagens no formato "TIFF". Como esse tipo de biblioteca nunca pede a autorização do usuário para abrir uma imagem, possíveis falhas em suas funções são facilmente exploráveis.

Chris Evans encontrou várias delas numa auditoria de código. Algumas das falhas são estouros de buffer, outras são estouros de inteiros e assemelhados. Essa falha foi classificada pelo CVE com o ID CAN-2004-0803.

Matthias Claasen também encontrou uma divisão por zero na libtiff. Essa falha foi classificada pelo CVE com o ID CAN-2004-0804.

Uma investigação mais aprofundada, levada a termo por Dmitry Levin, expôs inúmeros casos de estouro de inteiros. As falhas foram classificadas pelo CVE com o ID CAN-2004-0886.

A empresa iDEFENSE Security localizou, ainda, um estouro de buffer na manipulação de arquivos OJPEG (JPEG obsoleto) no pacote libtiff do SuSE Linux. O problema foi corrigido com a desativação sumária do suporte a OJPEG e foi classificado pelo CVE com o ID CAN-2004-0929. ■

Referência no Mandrake: MDKSA-2004:109
Referência no Red Hat: RHSA-2004:577-16
Referência no Slackware: SSA:2004-305-02
Referência no SuSE: SUSE-SA:2004:038

IPtables

Faheem Mitha observou que o comando *iptables*, uma ferramenta administrativa para o filtro de pacotes IPv4 e NAT do kernel do Linux, nem sempre carrega automaticamente todos os módulos necessários da forma como deveria. Com isso, algumas regras do firewall podem ficar inoperantes quando o sistema é ligado. Há relatos de que pelo menos o lokkit acusa problemas de conexão devido a essa falha.

Os usuários são aconselhados a atualizar os pacotes do iptables. ■

Referência no Debian: DSA-580-1 iptables
Referência no Mandrake: MDKSA-2004:125
Referência no SuSE: SUSE-SA:2004:037

Apache

O Servidor HTTP Apache é, sem dúvida, o mais popular servidor web da Internet. O mod_include é um módulo do Apache que adiciona recursos de scripts executados no servidor (Server Side Includes – SSI).

Um possível estouro de buffer foi identificado na função get_tag( ) do arquivo mod_include.c. Se os Server Side Includes (SSI) estiverem ativados, um invasor local poderia executar código arbitrário usando um documento especialmente preparado com SSI mal-formado. O código seria executado com as permissões do usuário dono do processo-filho do daemon httpd.

Um estouro de buffer baseado no segmento de dados (heap) também foi encontrado no módulo mod_proxy. Outo módulo, mod_ssl, foi atualizado da versão mod_ssl-2.8.19-1.3.31 para a versão 2.8.21-1.3.32. Isso corrige uma falha que permite a um cliente usar uma cifra que o servidor não considera segura o bastante.

Um novo pacote do PHP (php-4.3.9) também está disponível para várias outras plataformas.

Mais detalhes sobre todas essas falhas podem ser encontradas no "Common Vulnerabilities and Exposures" (cve.mitre.org – CAN-2004-0492 e CAN-2004-0885). ■

Referência no Gentoo: GLSA 200411-03 / apache
Referência no Mandrake: MDKSA-2004:122
Referência no Slackware: SSA:2004-305-01

Squid

O Squid é um servidor de proxy para Web com muitos recursos, entre eles o cache de conteúdo. A empresa iDEFENSE divulgou uma falha no módulo SNMP, que permite a um invasor reiniciar o servidor e derrubar conexões já abertas. Para isso, basta mandar pacotes arbitrários à porta SNMP. O projeto "Common Vulnerabilities and Exposures" (cve.mitre.org) deu a essa falha o código CAN-2004-0918. ■

Referência no Debian: DSA-576-1 squid
Referência no Gentoo: GLSA 200410-15 / squid
Referência no Mandrake: MDKSA-2004:112
Referência no Red Hat: RHSA-2004:591-04

Gaim

O Gaim é um aplicativo de mensagens eletrônicas instantâneas que reconhece inúmeros protocolos. Um estouro de buffer foi descoberto no manipulador (handler) do protocolo do MSN. Quando recebe uma seqüência inesperada de mensagens MSNSLP, é possível que um invasor possa travar o programa ou mesmo executar código arbitrário. O projeto "Common Vulnerabilities and Exposures" (cve.mitre.org) deu a essa falha o código CAN-2004-0891.

A atualização do programa também conserta uma quantidade razoável de problemas na interface gráfica, na decodificação de protocolos e no tratamento de erros, incluindo uma falha na codificação de comunicações com ICQ. ■

Referência no Gentoo: GLSA 200410-23 / gaim
Referência no Red Hat: RHSA-2004:604-05
Referência no Slackware: SSA:2004-239-01

ImageMagick

O ImageMagick™ é um programa para manipulação e exibição de imagens para o X Window System. Um estouro de buffer baseado no segmento de dados (heap) foi descoberto no descritor de imagens. Um invasor poderia criar um arquivo BMP cuidadosamente adulterado de forma a causar a execução de código arbitrário. O projeto "Common Vulnerabilities and Exposures" (cve.mitre.org) deu a essa falha o código CAN-2004-0827. ■

Referência no Red Hat: RHSA-2004:480-05
GLSA 200411-11 / imagemagick