Dicas de [In]segurança

Kerberos

O Kerberos é um sistema de autenticação em rede que utiliza Trusted Third Party (um KDC) para autenticar clientes e servidores entre si.

Vários erros double-free foram encontrados no KDC do Kerberos 5 e suas bibliotecas. Um invasor remoto pode potencialmente explorar essas falhas para executar código. O projeto Common Vulnerabilities and Exposures (*http://cve.mitre.org*) deu a esses problemas os códigos CAN-2004-0642 e CAN-2004-0643. Um erro double-free também foi encontrado no servidor krb524 (CAN-2004-0772).

Um loop infinito foi encontrado na biblioteca de decodificação do Kerberos 5 ASN.1. Um invasor remoto pode conseguir disparar essa falha e causar um ataque de negação de serviço (Denial of Service – DoS). O projeto Common Vulnerabilities and Exposures deu a esse problema o código CAN-2004-0644.

Ao tentar entrar em contato com um KDC, as bibliotecas do Kerberos irão iterar através da lista de servidores, tentando contatar um ao outro. Se um dos servidores deixar de responder, o cliente desiste e tenta contatar o próximo servidor da lista, repetindo o processo. Para aplicativos que precisam contatar um KDC muitas vezes, o acúmulo do tempo gasto na espera pode ser significativo.

Todos os usuários do krb5 devem instalar as atualizações referenciadas a seguir. ■

Código de Referência do Mandrake
MDKSA-2004:088
Código de Referência do Debian:
DSA-543-1
Código de Referência do Gentoo:
GLSA 200409-09 / mit-krb5
Código de Referência do Red Hat:
RHSA-2004:350-12

Qt

A Qt é uma biblioteca de software que simplifica a tarefa de escrever e manter aplicativos GUI (Graphical User Interface) para o sistema X Window.

Durante um exame de segurança, Chris Evans descobriu um estouro de pilha no decodificador de imagens BMP em versões da Qt anteriores à 3.3.3. Um invasor poderia criar um arquivo BMP especial, de forma que ele faça com que um aplicativo ligado à Qt caia ou possivelmente execute um código qualquer quando a imagem fosse aberta por uma vítima. O projeto Common Vulnerabilities and Exposures deu a esse problema o código CAN-2004-0691.

Além disso, várias falhas foram descobertas nos decodificadores GIF, XPM, e JPEG nas versões da Qt anteriores à 3.3.3. Um invasor poderia criar arquivos de imagens de uma forma que, quando abertos por uma vítima, pudessem fazer com que um aplicativo ligado à Qt caísse. O projeto Common Vulnerabilities and Exposures deu a esses problemas os códigos CAN-2004-0692 e CAN-2004-0693.

Usuários da Qt devem instalar os pacotes de atualização referenciados abaixo, que contêm correções e não são mais vulneráveis a esses problemas. ■

Código de Referência do Mandrake:
MDKSA-2004:085
Código de Referência do SuSE:
SUSE-SA:2004:027
Código de Referência do Slackware:
SSA:2004-236-01
Código de Referência do Debian:
DSA-542-1 qt -- unsanitised input
Código de Referência do Red Hat:
RHSA-2004:414-19

KDE

KDE é um dos mais populares ambientes de trabalho para sistemas Unix, entre eles o Linux.

A integridades dos links simbólicos usados pelo KDE não é garantida. Como conseqüência, isto pode ser mal utilizado por invasores locais para criar ou truncar arquivos ou impedir os aplicativos KDE de funcionarem corretamente (CAN-2004-0689).

O servidor DCOP cria arquivos temporários de uma maneira não segura. Esses arquivos temporários são utilizados para autenticação, então, potencialmente, poderiam permitir que um invasor local comprometa a conta de qualquer usuário executando um aplicativo KDE (CAN-2004-0690). Note que apenas a versão 3.2.x do KDE é afetada por essa vulnerabilidade.

O navegador web Konqueror permite que sites da Internet carreguem o conteúdo de outros sites dentro de um frame em suas páginas. Isso pode possibilitar a inserção de código e scripts maliciosos em um site aparentemente confiável. Esta vulnerabilidade tem o código CAN-2004-0721.

O navegador da web Konqueror também permite que websites criem cookies para certos domínios de primeiro nível específicos a cada país. Isso pode ser usado para fazer com que o Konqueror envie cookies para todos os outros websites operando sob o mesmo domínio, o que pode ser utilizado para criar um ataque de "session fixation". Todos os domínios secundários de primeiro nível com mais de dois caracteres na parte secundária do nome do domínio, caso ela seja diferente de com, net, mil, org, gov, edu ou int, são afetados (CAN-2004-0746). ■

Código de Referência do Mandrake:
MDKSA-2004:086
Código de Referência do Slackware:
SSA:2004-247-01
Código de Referência do Debian:
DSA-539-1 kdelibs -- temporary directory vulnerability

Apache

O servidor HTTP Apache é um servidor web poderoso, cheio de recursos, eficiente e livremente disponível.

Um erro de filtro de entrada no *mod_ssl* foi descoberto no daemon httpd versão 2.0.50 e anteriores. Um invasor remoto poderia forçar uma conexão SSL a ser abortada em determinado ponto e fazer com que um processo filho do Apache entre em loop infinito, consumindo recursos da CPU. O projeto Common Vulnerabilities and Exposures deu a esse problema o código CAN-2004-0748. A SuSE divulga a advertência CAN-2004-0751 para uma vulnerabilidade parecida.

A SuSE sugere que o problema seja contornado desabilitando o módulo mod_ssl no Apache, reiniciando o servi-

dor em seguida. Você pode também atualizar o pacote *libapr0* e um dos pacotes *apache2-prefork* ou *apache2-worker*, dependendo se você usa a configuração *-prefork* ou *-worker*. ■

Código de Referência do SuSE: SUSE-SA:2004:030
Código de Referência do Red Hat: RHSA-2004:349-10

rsync

O Programa rsync sincroniza arquivos através de uma rede.

Versões do rsync até (e inclusive) a 2.6.2 contêm um problema de "path sanitization". Esse problema pode permitir a um invasor ler ou gravar arquivos fora do diretório rsync. Essa vulnerabilidade é apenas explorável quando um servidor rsync não está rodando dentro de um ambiente *chroot*. O projeto Common Vulnerabilities and Exposures deu a esse problema o código CAN-2004-0792.

Usuários do rsync devem instalar em seus sistemas os pacotes atualizados referenciados abaixo, que não são mais afetados pelo problema. ■

Código de Referência do SuSE: SUSE-SA:2004:026
Código de Referência do Debian: DSA-538-1 rsync -- unsanitised input processing
Código de Referência do Red Hat: RHSA-2004:436-07

PNG

Várias falhas de segurança foram encontradas na biblioteca PNG, utilizada por aplicativos para dar suporte ao formato de imagem PNG.

Chris Evans informa que um invasor remoto poderia executar código ao disparar um buffer overflow devido à manipulação incorreta do comprimento dos dados no campo transparency chunk e em outros pontos do processamento de imagens. (VU#388984, VU#817368, CAN-2004-0597) Uma imagem PNG especial pode ser usada para fazer com que um aplicativo caia devido a uma referência a um ponteiro nulo na função *png_handle_iCPP()* (e em outros locais). (VU#236656, CAN-2004-0598) *Integer overflows* foram encontrados nas funções *png_handle_sPLT()*, *png_read_png()* e outros locais. Esses erros podem, no mínimo, fazer um aplicativo cair, e tem referências VU#160448, VU#477512, VU#286464 e CAN-2004-0599. ■

Código de Referência SuSE: SUSE-SA:2004:023
Código de Referência Slackware: SSA:2004-222-01

Acrobat

O navegador Adobe Acrobat Reader permite a visualização, distribuição, e impressão de documentos no formato PDF (Portable Document Format).

O iDEFENSE informou que o Adobe Acrobat Reader 5.0 contêm um buffer overflow ao decodificar documentos uuencoded. Um invasor pode executar código arbitrário na máquina de uma vítima se ela abrir um documento uuencoded especialmente construído.

Esse problema apresenta risco de execução remota, uma vez que o Acrobat Reader geralmente é o manipulador padrão para arquivos PDF. O projeto Common Vulnerabilities and Exposures deu a esse problema o código CAN-2004-0631.

O iDEFENSE também noticiou que o Adobe Acrobat Reader 5.0 contém um erro de validação de entrada ao lidar com documentos "uuencoded". Um invasor poderia criar um arquivo com um nome especialmente formulado que poderia levar a execução de um comando qualquer na máquina de uma vítima. O projeto Common Vulnerabilities and Exposures deu a esse problema o código CAN-2004-0630.

Recomenda-se que todos os usuários do Acrobat Reader atualizem o programa. ■

Código de Referência do Red Hat: RHSA-2004:432-08

zlib

A zlib é uma biblioteca de compressão de dados amplamente utilizada. Entre os programas ligados a ela estão muitos aplicativos desktop, assim como servidores como o Apache e o OpenSSH.

A função *inflate* da zlib lida com certos dados de entrada incorretamente, o que pode levar a uma condição de negação de serviço (Denial of Service) em programas que a utilizam com dados não confiáveis. Se a vulnerabilidade pode ser explorada local ou remotamente, depende do aplicativo que o utiliza.

Versões da zlib posteriores à 1.2 não são afetadas. Não se conhece nenhuma forma de contornar o problema. Depois de aplicar a atualização, todos os programas ligados à zlib devem ser reiniciados. ■

Código de Referência Mandrake: MDKSA-2004:090
Código de Referência SuSE: SUSE-SA:2004:028

Gaim

O Gaim é um cliente de mensagens instantâneas capaz de lidar com múltiplos protocolos, como ICQ, AIM e MSN.

Erros de buffer overflow foram achados no suporte ao protocolo MSN. Para poder explorar estes erros, um invasor teria que interceptar os dados entre o servidor MSN e um cliente vulnerável. Isto poderia permitir a execução de código. O projeto Common Vulnerabilities and Exposures deu a esse problema o código CAN-2004-0500.

Erros de buffer overflow também foram encontrados no decodificador de URLs do Gaim, na resolução do hostname local e no interpretador de mensagens RTF. Um invasor remoto pode enviar um pacote IP especialmente construído para um cliente vulnerável e levar à queda do programa ou execução de código. O projeto Common Vulnerabilities and Exposures deu a esse problema o código CAN-2004-0785.

Um erro de "shell escape" foi encontrado no arquivo de instalação de *smileys* do Gaim. Quando um usuário instala este tipo de tema, a descompactação dos dados é feita de uma forma insegura. Um invasor poderia criar um conjunto malicioso de smileys que executaria comandos quando fosse instalado pela vítima. O projeto Common Vulnerabilities and Exposures deu a esse problema o código CAN-2004-0784.

Um *integer overflow* foi encontrado na rotina de recepção de mensagens do Gaim Groupware. É possível que, se o usuário se conectar a um servidor comprometido, um invasor envie um pacote de dados construido de forma a possibilitar a execução de código na máquina da vítima. O projeto Common Vulnerabilities and Exposures deu a esse problema o código CAN-2004-0754. ■

Código de Referência SuSE: SUSE-SA:2004:023
Código de Referência Slackware: SSA:2004-239-01
Código de Referência Red Hat: RHSA-2004:400-15