Dicas de [In]segurança

krb5

O *Kerberos* é um sistema de autenticação em rede que usa um terceiro elemento confiável, chamado KDC, para autenticar os clientes e servidores, fazendo as correspondências entre eles.

O pacote *krb5-workstation* inclui um cliente *Telnet* já preparado para autenticação via Kerberos. Dois estouros de buffer foram descobertos na maneira como o cliente de Telnet trata as mensagens vindas do servidor. Um invasor poderia executar código arbitrário na máquina da vítima se puder persuadi-la a conectar-se a um servidor Telnet malicioso. O projeto "Common Vulnerabilities and Exposures" (cve.mitre.org) deu a essa falha os códigos CAN-2005-0468 e CAN-2005-0469. ■

Referência no Debian: DSA-703-1 krb5

Referência no Gentoo: GLSA 200504-04 / telnet

Referência no Mandriva: MDKSA-2005:061

Referência no Red Hat: RHSA-2005:330-06

MySQL

O *MySQL* é um servidor de banco de dados SQL multitarefa e multiusuário.Esta atualização repara inúmeras situações de risco no servidor MySQL.

Stefano Di Paola descobriu duas falhas na maneira como o MySQL manipula funções definidas pelo usuário. Um agressor poderia criar e executar funções definidas por ele próprio, levando à execução de código arbitrário no servidor MySQL. O projeto "Common Vulnerabilities and Exposures" (cve.mitre.org) deu a essa falha os códigos CAN-2005-0709 e CAN-2005-0710.

Di Paola também encontrou uma falha na maneira como o MySQL cria tabelas temporárias. Um usuário local poderia criar um link simbólico especialmente preparado de forma a ludibriar o MySQL, fazendo-o sobrescrever um arquivo para o qual tenha permissão de escrita. O projeto "Common Vulnerabilities and Exposures" (cve.mitre.org) deu a essa falha o código CAN-2005-0711. ■

Referência no Gentoo: GLSA 200503-19 / mysq

Referência no Mandriva: MDKSA-2005:060

Referência no Red Hat: RHSA-2005:334-07

Referência no SuSE: SUSE-SA:2005:019

Telnet

O pacote *telnet* oferece um cliente em modo texto para o protocolo Telnet. O pacote *telnet-server* inclui um *daemon* de um servidor de Telnet – o *telnetd* – que permite logins remotos na máquina em que roda.

Dois estouros de buffer foram encontrados no cliente, na rotina de tratamento de mensagens vindas do servidor. Um invasor poderia executar código na máquina da vítima se ela puder ser persuadida a conectar-se a um servidor Telnet malicioso. O projeto "Common Vulnerabilities and Exposures" (cve.mitre.org) deu a essa falha os códigos CAN-2005-0468 e CAN-2005-0469. ■

Referência no Debian: DSA-703-1 krb5

Referência no Gentoo: GLSA 200504-04 / telnet

Referência no Red Hat: RHSA-2005:327-10

Mozilla

O *Mozilla* é um conjunto de programas de código aberto para a Internet que inclui um navegador Web, um poderoso cliente de email, um leitor de grupos de discussão (*newsgroups*), um programa para bate-papo em salas na Internet pelo protocolo IRC e um editor de HTML.

Há um estouro de buffer na maneira como o Mozilla processa imagens GIF. Um invasor poderia facilmente criar uma imagem GIF especialmente manipulada que, quando aberta dentro do Mozilla pela vítima, permitiria a execução de código arbitrário. O projeto "Common Vulnerabilities and Exposures" (cve.mitre.org) deu a essa falha o código CAN-2005-0399.

Uma falha foi encontrada na maneira como o Mozilla exibe caixas de diálogo. Em situações em que diversas páginas estejam abertas em abas, uma página maliciosa que esteja numa aba não ativa (ou seja, que não esteja sendo mostrada) poderia apresentar ao usuário uma caixa de diálogo, levando-o a acreditar que essa caixa pertence à página ativa (ou seja, à página que o usuário está lendo no momento). O projeto "Common Vulnerabilities and Exposures" (cve.mitre.org) deu a essa falha o código CAN-2004-1380.

Há ainda outra falha, desta vez na maneira como o Mozilla autoriza os plugins a carregar conteúdo privilegiado em um *frame* HTML (com a *tag* <*frame*>). A falha permite que uma página insidiosa possa persuadir o usuário a clicar em certos lugares, o que poderia provocar a reconfiguração do sistema ou mesmo a execução de código arbitrário. O projeto "Common Vulnerabilities and Exposures" (cve.mitre.org) deu a essa falha o código CAN-2005-0232.

Não é só o navegador que possui problemas. Um comportamento anormal no *Mozilla Mail*, mais precisamente nas rotinas que tratam os famigerados *cookies*, pode causar dores de cabeça. Ao receber os cookies quando carrega conteúdo sobre o protocolo HTTP – por exemplo, um email em HTML com um frame que carrega uma página externa –, o Mozilla Mail tende a não respeitar as configurações do usuário quanto à forma de manipulá-los. É possível rastrear um usuário com o uso de mensagens de email maliciosas que carregam conteúdo por HTTP. O projeto "Common Vulnerabilities and Exposures" (cve.mitre.org) deu a essa falha o código CAN-2005-0149.

O Mozilla faz das suas também na forma como responde a solicitações para autenticação em servidores de proxy. Um servidor web malicioso poderia roubar credenciais

do navegador da vítima se emitir uma resposta do tipo 407 (*proxy authentication request*, ou *solicitação de autenticação via proxy*). O projeto "Common Vulnerabilities and Exposures" (cve.mitre.org) deu a essa falha o código CAN-2005-0147.

As rotinas de validação tags HTML também tem problemas. Algumas tags de início, se seguidas pelo caracter NULL, podem tirar o navegador de sua órbita. Uma página maliciosamente preparada poderia travar o Mozilla assim que a vítima tentasse abrí-la. O projeto "Common Vulnerabilities and Exposures" (cve.mitre.org) deu a essa falha o código CAN-2004-1613.

Uma falha foi encontrada na forma como o Mozilla lida com as permissões para a instalação de pacotes XPI – a maioria das extensões e temas, bem como alguns dos plugins do Mozilla, são distribuídos nesse formato. É possível que um pacote XPI deixe alguns dos arquivos com permissão de leitura (ou escrita) para todos os usuários do computador, permitindo que qualquer usuário local possa roubar dados sigilosos ou executar código arbitrário. O projeto "Common Vulnerabilities and Exposures" (cve.mitre.org) deu a essa falha o código CAN-2004-0906.

Uma falha foi encontrada na forma como o Mozilla abre novas abas cada vez que se "clica" com o botão do meio em algum link. Uma página maliciosa poderia ler arquivos locais ou ou reconfigurar o *chrome*. O projeto "Common Vulnerabilities and Exposures" (cve.mitre.org) deu a essa falha o código CAN-2005-0141.

E a última do mês para o Mozilla. Uma falha foi encontrada na maneira como o programa mostra o ícone indicador de site seguro. Um site malicioso poderia carregar, em segundo plano, uma página realmente segura enquanto exibe na tela uma página com truques para enganar, de alguma forma, o usuário. Como está carregando "por trás" uma página segura, o Mozilla irá mostrar o ícone de site seguro, embora a página sendo exibida não o seja. O projeto "Common Vulnerabilities and Exposures" (cve.mitre.org) deu a essa falha o código CAN-2005-0144. ■

Referência no Gentoo: GLSA 200503-30 / Mozilla

Referência no Red Hat: RHSA-2005:323-10

❒ gtk2

O pacote *gtk2* contém o famoso *GIMP ToolKit* (GTK+), uma biblioteca com funções para criar interfaces gráficas que funcionem sob o X Window System.

Uma falha foi encontrada na maneira como o GTK 2 processa imagens BMP. É possível usar imagens BMP especialmente manipuladas para causar uma negação de serviço no aplicativo que usa essa biblioteca. O projeto "Common Vulnerabilities and Exposures" (cve.mitre.org) deu a essa falha o código CAN-2005-0891. ■

Referência no Mandriva: MDKSA-2005:068

Referência no Red Hat: RHSA-2005:344-03z

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.*