# Dicas de [In]segurança

## Emacs

O *Emacs* é um editor de texto poderoso, altamente personalizável, auto-documentador e independente de arquitetura.

Max Vozeler descobriu diversas vulnerabilidades de formatação de cadeias de caracteres (*strings*) no utilitário *movemail* do Emacs. Se um usuário se conectasse a um servidor POP malicioso, um agressor poderia executar código arbitrário com as permissões do usuário que estivesse rodando o Emacs. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2005-0100.

Todos os usuários do Emacs são aconselhados a atualizar o programa para a versão mais nova. ■

Referência no Gentoo: GLSA 200502-20 / Emacs

Referência no Mandrake: MDKSA-2005:038

Referência no Red Hat: RHSA-2005:110-06

Referência no SUSE: SUSE-SR:2005:006

## Squid

O *Squid* é um proxy para a web desenvolvido para sistemas Unix.

Um estouro de buffer foi encontrado no interpretador *Gopher*. Essa falha permite que um servidor Gopher remoto possa derrubar um proxy Squid que leia dados a partir dele. Embora os servidores Gopher sejam bastante raros hoje em dia, uma página web maliciosa (por exemplo) poderia redirecionar o usuário ao site

### Postura das principais distribuições Linux quanto à segurança

| Distribuição | Referência de Segurança | Comentários |
|---|---|---|
| **Conectiva** | Info: http://distro2.conectiva.com.br/<br>Lista: seguranca-admin@distro.conectiva.com.br e http://distro2.conectiva.com.br/lista/<br>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/<br>Lista: http://lists.debian.org/debian-security-announce/<br>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<br>Fórum: http://forums.gentoo.org/<br>Lista: http://www.gentoo.org/main/en/lists.xml<br>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<br>Lista: http://www.mandrakesecure.net/en/mlist.php<br>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/<br>Lista: http://www.redhat.com/mailing-lists/<br>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/<br>Lista: http://www.slackware.com/lists/ (slackware-security)<br>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/<br>Lista: http://www.novell.com/linux/download/updates/<br>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.*

Gopher malicioso, ou conter um quadro (*frame*) apontando para esse site. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2005-0094.

Uma falha de estouro de inteiros foi encontrada no interpretador de mensagens WCCP. É possível derrubar o Squid se o agressor for capaz de enviar uma mensagem WCCP mal-formada com um endereço de origem "falsificado" (*spoofed*) que remeta ao *home router* do Squid. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2005-0095.

Também no interpretador WCCP foi encontrado um estouro de buffer. O resultado é o usual: um agressor pode mandar pacotes malformados que tirariam o Squid do ar ou, o que é pior, permitiriam executar código arbitrário. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2005-0211.

Um vazamento de memória foi encontrado no módulo de autenticação *NTLM fakeauth_auth*. Um agressor poderia colocar o servidor Squid sob uma carga pesadíssima de tráfego, obrigando o módulo a consumir uma quantidade fabulosa de memória, resultando numa negação de serviço (*Denial of Service*, ou DoS). O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2005-0096.

Uma falha de derreferência a um ponteiro nulo (*NULL pointer*) foi encontrada também no módulo *NTLM fakeauth_auth*. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2005-0097.

Foi encontrada uma falha de validação de usuário no módulo *squid_ldap_auth*. A falha permite que se "estufe" o nome do usuário com espaços em branco. Com isso, é possível contornar regras explícitas de controle de acesso ou tirar proveito de uma administração de usuários confusa. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2005-0173.

A maneira como o Squid trata as respostas a requisições HTTP precisa de retrabalho. Como está hoje, um servidor web malicioso poderia enviar uma série de respostas HTTP especialmente manipuladas para "envenenar" o cache do Squid. Com o cache envenenado, os usuários podem ser remetidos a páginas diferentes das que eles pediram – e isso pode ser usado em benefício do agressor. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha dois códigos: CAN-2005-0174 e CAN-2005-0175.

Em outra falha semelhante, o Squid não consegue tratar corretamente cabeçalhos HTTP muito grandes em respostas a requisições. Um servidor web malicioso poderia enviar um cabeçalho especialmente criado para – novamente – envenenar o cache do Squid. O resultado é o mesmo: com o cache envenenado, os usuários podem ser remetidos a páginas diferentes das que pediram. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2005-0241. ■

Referência no Debian: DSA-688-1 squid
Referência no Gentoo: GLSA 200502-25 / Squid
Referência no Mandrake: MDKSA-2005:047
Referência no Red Hat: RHSA-2005:060-20
Referência no SUSE: SUSE-SA:2005:008

## ❒ Firefox

O *Mozilla Firefox* é um navegador de Internet de código aberto e livre.

Foi encontrada uma falha nas funções de manipulação de cadeias de caracteres (ou *strings*) do Firefox. Se um site malicioso puder usar isto para exaurir a memória na máquina do cliente, seria possível executar código arbitrário. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2005-0255. ➡

Outra falha foi encontrada, desta vez no tratamento de janelas *pop-up*, tornando possível que um site malicioso controle o conteúdo de uma janela pop-up de um *outro* site. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2004-1156.

Há um *bug* na maneira como o Firefox permite que os *plug-ins* adicionem conteúdo a um *frame*. É possível que uma página maliciosa induza o usuário a clicar em certos lugares para modificar configurações ou executar código arbitrário. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha os códigos CAN-2005-0232 e CAN-2005-0527.

Outra falha também grave: um atacante poderia explorar a forma como o Firefox mostra os domínios internacionais – como, por exemplo, .co.uk, .org.br e .edu.af. É possível que o agressor mostre uma URL válida, mas que aponte para outra página que não a correta. O usuário pensa que está vendo a página legítima mas está, na realidade, visitando uma impostora. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2005-0233.

Uma falha do tipo "espírito de porco": a maneira como o Firefox trata os arquivos temporários dos plug-ins pode permitir que um usuário apague arquivos de outro. Por exemplo, um agressor local poderia criar links simbólicos na pasta /tmp que apontem para o diretório pessoal (/home) da vítima. Quando o Firefox for finalizado, os arquivos no /home da vítima são apagados. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2005-0578.

Os conversores de UTF-8 do Firefox também estão infestados de baratas. Um agressor poderia enviar uma cadeia de caracteres UTF-8 especialmente formulada ao conversor, levando à execução de código arbitrário. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2005-0592.

Nem o gerenciador de segurança de javascript do Firefox escapa. Se um usuário arrasta e solta um link malicioso para uma aba, o gerenciador é contornado. Com isso, é possível executar código remotamente ou conseguir informações sigilosas. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2005-0231.

O prompt de autenticação (usuário e senha) do Firefox também tem problemas. Quando o usuário entra em uma página privada e é instado a informar seu nome e sua senha, a caixa de diálogo é mostrada sobre a aba ativa, não importando qual aba disparou o pedido de nome e senha. Isso pode ser usado para enganar o usuário, fazendo com que ele dê o nome e senha de um site real, embora a caixa de diálogo tenha sido disparada por um site malicioso. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2005-0584.

Outro problema em caixas de diálogo: a janela *Salvar arquivo* permite que um site malicioso manipule o cabeçalho *Content-Disposition*, fazendo com que o usuário pense que está baixando um arquivo de tipo diferente do que ele realmente está baixando – por exemplo, o usuário pode ser levado a pensar que está baixando um MP3 quando na verdade é um executável do Windows. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2005-0586.

Também há falhas no sistema de auto-completar do Firefox, usando as setas de direção do teclado. Quando uma opção do auto-completar é selecionada, a informação é copiada no controle de entrada. Um site malicioso poderia roubar informações do usuário se puder induzi-lo a escolher certas opções. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2005-0589.

Não uma, mas várias falhas foram encontradas na rotina que mostra o ícone de sites seguros. Um site malicioso poderia forçar a exibição do ícone seguro mesmo que os certificados de criptografia estejam incorretos. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2005-0593.

Há um *bug* na maneira como o Firefox mostra a caixa de diálogo de download. Um site malicioso poderia encobrir a URL a partir da qual o conteúdo está sendo baixado, fazendo o usuário acreditar que ele vem de um site confiável e conhecido – quando, na verdade, está vindo de um site suspeito. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2005-0585.

Mais um: há uma falha de interpretação no processamento das diretivas *xsl:include* e *xsl:import*. É possível que sites maliciosos importem folhas de estilo XSLT de um domínio atrás de um firewall, permitindo que um atacante obtenha informações sigilosas. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2005-0588.

Outra falha foi encontrada na maneira como o Firefox mostra a caixa de diálogo de confirmação de instalação. Um agressor poderia adicionar uma cadeia de caracteres no formato *usuario:senha*, escondendo o nome real do site de onde se está baixando o conteúdo a ser instalado. Com isso, o usuário pode ser levado a pensar que está instalando algo de um site confiável. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2005-0590.

Uma última falha foi encontrada na maneira como o Firefox mostra caixas de diálogo de downloads e de segurança. Um agressor poderia cobrir parte delas, podendo assim enganar o usuário e levá-lo a clicar em *Allow* (*Permitir*) ou *Open* (*Abrir*), o que poderia permitir a execução de código. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu o código CAN-2005-0591 a esta falha. ■

Referência no Gentoo: GLSA 200503-10 / Firefox

Referência no Red Hat: RHSA-2005:176-11