Dicas de [In]segurança

OpenOffice.org

O *OpenOffice.org* é um conjunto de aplicativos para escritório que inclui um processador de textos, uma planilha eletrônica, um gerenciador de apresentações, um editor de fórmulas e um programa para criação e edição de desenhos e gráficos vetoriais.

Um estouro de buffer baseado no segmento de dados (*heap*) foi encontrado no processador de documentos do Microsoft Word do OpenOffice.org. Um agressor poderia criar um documento no formato DOC especialmente manipulado para forçar o OpenOffice.org a executar código arbitrário no momento em que o arquivo fosse aberto. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2005-0941.

Todos os usuários do OpenOffice.org são aconselhados a atualizar o programa. ■

Referência no Gentoo: GLSA 200504-13 / OpenOffice

Referência no Mandriva: MDKSA-2005:082

Referência no Red Hat: RHSA-2005:375-07

Referência no SuSE: SUSE-SA:2005:025

RealPlayer

O *RealPlayer* é um *media player* que trabalha com arquivos locais e *streaming*. Reproduz os formatos RealAudio, RealVideo, MP3, 3GPP, Flash, SMIL 2.0, JPEG, GIF, PNG, RealPix, RealText e outros.

Um estouro de buffer foi encontrado no modo como o RealPlayer processa arquivos RAM. Um agressor poderia criar um arquivo RAM manipulado para executar código arbitrário quando aberto pelo usuário. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2005-0755.

Todos os usuários do RealPlayer são aconselhados a atualizar o programa. ■

Referência no Gentoo: GLSA 200504-21 / RealPlayer

Referência no Red Hat: RHSA-2005:363-10

Referência no SuSE: SUSE-SA:2005:026

Firefox

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

Vladimir V. Perepelitsa descobriu uma falha na maneira com que o Firefox manipula funções anônimas durante a interpretação de expressões regulares. É possível que uma página web maliciosa possa ser capaz de capturar um bloco qualquer da memória usada pelo navegador, podendo levar a revelação de dados sigilosos do usuário ou do sistema. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2005-0989.

Omar Khan descobriu uma falha na maneira como o Firefox processa a *tag PLUGINSPAGE*. É possível que uma página com segundas intenções persuada o usuário a clicar no botão *Instalação manual* (*Manual install*) de um plugin desconhecido, levando à execução de código arbitrário na linguagem *JavaScript*. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2005-0752.

Mais uma: Doron Rosenberg descobriu uma falha na maneira como o Firefox mostra as janelas de pop-up. Se um usuário escolher clicar numa janela cuja URL não passa de código JavaScript malévolo, o script será executado com privilégios elevados. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2005-1153.

A lista é interminável. Uma falha foi encontrada na maneira como o Firefox encara o escopo global para o JavaScript em uma dada janela. É possível que uma página maliciosa defina uma variável global que sabidamente é usada por outro site, permitindo que código imundo seja executado no contexto do site inocente. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2005-1154.

Michael Krax descobriu um *bug* na maneira como o Firefox lida com os *favicons*, ícones que representam um website. Um site poderia aplicar o truque sujo de definir a URL do favicon como um código em JavaScript, que poderia fazer muito mais coisas além de exibir o pequeno ícone na barra de endereços. O código arbitrário executado teria privilégios altos no sistema. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2005-1155.

Krax encontrou baratas até mesmo na maneira como o Firefox instala plugins de busca. Se um usuário escolher instalar um deles a partir de um site suspeito, o novo plugin pode, silenciosamente, substituir um plugin existente. Com isso, o plugin facínora poderia executar código arbitrário e roubar informações secretas. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha os códigos CAN-2005-1156 e CAN-2005-1157.

Kohei Yoshino descobriu ninhos de traças na rotina de abertura de links da barra lateral do Firefox. Um site malicioso poderia construir um link de tal forma que, quando clicado, executasse código JavaScript com privilégios elevados. O

projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2005-1158.

Uma falha foi encontrada na validação de objetos *XPInstall* (como extensões) em JavaScript pelo Firefox. Uma página com más intenções poderia passar outros objetos que seriam instalados "de carona" junto com um objeto XPInstall legítimo, levando o interpretador de JavaScript a saltar para posições arbitrárias na memória. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2005-1159.

Para passar a régua este mês: na janela de conteúdo, os nós DOM controlados por código na interface com o usuário (normalmente executados com privilégios altos) estão totalmente esburacados. Os rombos podem ser usados por páginas agressivas para instalar código JavaScript letal ou roubar dados do usuário. Tudo o que o incauto usuário precisa fazer é clicar em algum link ou abrir um menu de contexto – coisas que todos os internautas fazem e que não deveriam apresentar qualquer risco. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2005-1160.

Todos os usuários do Firefox são aconselhados a atualizar o programa. ■

Referências no Gentoo:
GLSA 200504-18 e GLSA 200505-11 / mozilla
Referência no Mandriva: MDKSA-2005:088
Referência no Red Hat: RHSA-2005:383-07
Referências no Slackware:
SSA:2005-111-04 e SSA:2005-135-01
Referência no SuSE: SUSE-SA:2005:028

Ethereal

O *Ethereal* é um analisador de protocolos de rede simples, mas riquíssimo em recursos e possibilidades de uso.

Há inúmeras vulnerabilidades nas versões do Ethereal anteriores a 0.10.11:

- Os "dissecadores" dos protocolos ANSI A e DHCP são vulneráveis a cadeias mal formadas de caracteres;
- Os "dissecadores" DISTCC, FCELS, SIP, ISIS, CMIP, CMP, CMS, CRMF, ESS, OCSP, PKIX1Explitit, PKIX Qualified, X.509, Q.931, MEGACO, NCP, ISUP, TCAP e Presentation estão vulneráveis a estouros de buffer.
- Os "dissecadores" dos protocolos KINK, WSP, SMB Mailslot, H.245, MGCP, Q.931, RPC, GSM e SMB NETLOGON estão vulneráveis a erros na administração dos ponteiros;
- Os "dissecadores" LMP, KINK, MGCP, RSVP, SRVLOC, EIGRP, MEGACO, DLSw, NCP e L2TP estão vulneráveis a problemas com loops infinitos;
- Os "dissecadores" Telnet e DHCP podem "capotar" sem aviso prévio;

- Os "dissecadores" TZSP, Bittorrent, SMB, MGCP e ISUP podem causar uma falha de segmentação;
- Os "dissecadores" dos protocolos WSP, 802.3 Slow protocols, BER, SMB Mailslot, SMB, NDPS, IAX2, RADIUS, SMB PIPE, MRDISC e TCAP podem ser levados a indicar falsos resultados;
- Os "dissecadores" dos protocolos DICOM, NDPS e ICEP são vulneráveis a erros de manipulação de memória;
- Os "dissecadores" dos protoclos GSM MAP, AIM, Fibre Channel, SRVLOC, NDPS, LDAP e NTLMSSP podem, também, sair do ar de uma hora para a outra sem motivo aparente.

Um agressor poderia usar uma (uma só basta) dessas 69 vulnerabilidades para derrubar o programa e executar código arbitrário com as permissões do usuário rodando o Ethereal, que poderia ser (e normalmente é) o próprio root. As falhas são extremamente preocupantes porque não há meios de usar nenhum tipo de "farejador" (ou *sniffer*) sem que se possua permissões de root. ■

Referência no Debian: DSA-718-2 ethereal

Referência no Gentoo: GLSA 200505-03 / Ethereal

Referência no Mandriva: MDKSA-2005:083

❒ CVS

O CVS (*Concurrent Version System*) é um dos sistemas para controle de versões mais populares entre projetos Open Source. Um estouro de buffer foi encontrado na maneira como o cliente do CVS processa informações de versão e autor. Se o usuário puder ser ludibriado para entrar em um servidor CVS mal intencionado, seria possível executar código arbitrário. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2005-0753.

Para piorar a situação, outro artrópode peludo e gosmento foi encontrado, envolvendo um ponteiro inválido que seria liberado acidentalmente pelo CVS. Entretanto, essa falha não parece ser explorável, e portanto não representa um risco de segurança.

Recomenda-se que todos os usuários do CVS atualizem suas cópias do programa. Mais informações podem ser encontradas nos boletins de segurança abaixo. ■

Referência no Debian: DSA-715-1 cvs

Referência no Gentoo: GLSA 200504-16 / CVS

Referência no Mandriva: MDKSA-2005:073

Referência no Red Hat:RHSA-2005:387-06

Referência no Slackware: SSA:2005-111-01

Referência no SuSE: SUSE-SA:2005:024

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.*