# Dicas de [In]segurança

## Samba

O Samba oferece serviços de compartilhamento de arquivos e impressoras a clientes SMB/CIFS, comumente estações de trabalho rodando o sistema operacional Microsoft Windows®.

Greg MacManus, dos iDEFENSE Labs, descobriu uma falha de estouro de inteiros em versões do Samba anteriores à 3.0.10. Um usuário remoto autenticado poderia explorar essa falha, que pode levar a execução de código arbitrário no servidor Samba. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2004-1154. Os usuários do Samba devem atualizar seu sistema. ■

Referência no Gentoo: GLSA 200412-13 / Samba
Referência no Mandrake: MDKSA-2004:158
Referência no Red Hat: RHSA-2004:670-10
Referência no SuSE: SUSE-SA:2004:045

## Zip

O *zip* é um utilitário de arquivamento capaz de criar arquivos compactados compatíveis com o popular formato de compressão ZIP.

Uma falha de estouro de buffer foi descoberta no *zip* ao lidar com nomes de arquivo longos. Um atacante poderia criar um caminho longo o bastante para derrubar o *zip* ou executar instruções arbitrárias. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2004-1010. ■

Referência no Debian: DSA-624-1
Referência no Red Hat: RHSA-2004:634-08

## nfs-utils

O pacote nfs-utils possui um daemon para o servidor NFS do kernel e ferramentas relacionadas, o que permite um nível de desempenho muito mais elevado do que com o servidor NFS tradicional do Linux, utilizado pela maior parte dos usuários.

Esse pacote contém também o programa *showmount*. O *showmount* busca, no daemon de montagem num host remoto, informações sobre o servidor NFS (*Network File System* – Sistema de Arquivos em Rede).

A SGI relatou que o daemon *stadt* não manejava corretamente o sinal SIGPIPE. Um cliente mal-configurado ou malicioso poderia derrubar o *stadt*, levando a uma negação de serviço. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2004-1014.

Arjan van de Ven descobriu um estouro de buffer no *rquotad*. Em arquiteturas de 64 bits, uma conversão de inteiros imprópria pode levar a um estouro de buffer. Um atacante com acesso a um volume compartilhado por NFS poderia enviar um pedido que levaria à execução de código arbitrário. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2004-0946. ■

Referência no Gentoo: GLSA 200412-08 / nfs-utils
Referência no Red Hat: RHSA-2004:583-09

## PHP

O PHP é uma linguagem de script embutida em páginas HTML, comumente usada em conjunto com o servidor HTTP Apache.

Falhas que possibilitam a revelação de informações sigilosas, liberação redundante de memória e subcarga (*underflow*) com referência negativa em uma matriz foram encontradas no código de desserialização do PHP. Muitos aplicativos usam a função *unserialize* em dados não-confiáveis do usuário, o que pode levar à execução de código arbitrário ou, pelo menos, ganhar acesso à memória. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2004-1019.

Foi encontrada uma falha na extensão *exif* (Exchangeable Image Format) do PHP, que leva a um estouro de buffer baseado na pilha (*stack*). Um atacante poderia criar um arquivo de imagem de tal maneira que, se fosse analisado por um script PHP usando a extensão *exif*, poderia derrubar o sistema ou potencialmente executar código arbitrário. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2004-1065.

Uma falha que revela informações sigilosas sobre o usuário foi descoberta na análise de variáveis "GPC" em PHP (*query strings*, *cookies* ou dados de um formulário enviados pelo método POST). Se algum script usasse os valores das variáveis GPC, seria possível revelar ao cliente porções de memória usadas pelo processo-filho *httpd*. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2004-0958.

Uma falha de acesso a arquivos foi descoberta na análise de formulários "multipart/form-data", usados por scripts PHP, que permite *upload* de arquivos. Em certas configurações, alguns scripts podem permitir que um cliente malicioso carregue arquivos para um diretório arbitrário em que o usuário "apache" tenha acesso de escrita. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2004-0959.

Encontraram-se falhas nas funções *shmop_write*, *pack* e *unpack* do PHP. Normalmente o usuário não passa valores a essas funções, portanto seria necessário um script malicioso em PHP especialmente preparado para explorar a falha. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2004-1018.

Inúmeras falhas foram encontradas no uso da chamada de sistema *select* no PHP, que poderiam ser disparadas se o PHP estiver rodando num Apache em que o número de arquivos abertos (como por exemplo os arquivos de log dos hosts virtuais) excedesse o limite padrão para os processos, que é de 1024. Alguns "remendos" provisórios foram incluídos para contornar esses problemas.

O script *phpize*, escrito em shell, é um utilitário incluído na distribuição do PHP e pode ser usado para construir extensões (módulos). Foi descoberta uma falha na montagem delas em algumas plataformas de 64 bits que impedem seu funcionamento correto.

O módulo de extensão *pcntl* é agora habilitado por padrão na linha de comando do interpretador PHP, `/usr/bin/php`. Esse módulo permite o controle de processos com chamadas como *fork* e *kill* de dentro do próprio script PHP. ■

Referência no Gentoo: GLSA 200412-14 / PHP

Referência no Red Hat: RHSA-2004:687-05

## Kernel

O kernel do Linux desempenha as funções básicas do sistema operacional.

Este relatório inclui correções para inúmeras falhas de segurança.

Petr Vandrovec descobriu uma falha na emulação de 32 bits, afetando o kernel 2.4 na arquitetura AMD64. Um agressor local poderia usar essa falha para conseguir mais privilégios. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2004-1144.

A ISEC Security Research descobriu diversas vulnerabilidades na funcionalidade IGMP, que foi trazida (*backported*) para os kernels do Red Hat Enterprise Linux 3. Essas falhas permitem que um usuário local provoque uma negação de serviço (travamento do programa) ou potencialmente ganhe mais privilégios. Se houver aplicativos que usem *multicast* sendo executados, essa falha também permite que usuários remotos derrubem o sistema. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2004-1137.

Em um outro alerta, tanto a ISEC Security Research como Georgi Guninski – trabalhando independentemente – descobriram uma falha na função *scm_send* na camada de mensagens auxiliares. Um usuário local poderia criar uma mensagem auxiliar especialmente preparada que possivelmente causaria uma negação de serviço (travamento do sistema). O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2004-1016.

Um vazamento de informações em ponto flutuante foi descoberto no código de mudança de contexto para a arquitetura ia64. Um usuário local poderia usar essa falha para ler valores de outros processos nos registros do processador quando o bit MFH fosse ligado. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2004-0565.

Kirill Korotaev encontrou uma falha na função *load_elf_binary* afetando kernels anteriores à versão 2.4.26. Um usuário local poderia criar um binário executável especialmente preparado, de forma a causar uma negação de serviço (travamento do sistema). O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2004-1234. ■

Referência no Red Hat: RHSA-2004:689-06

Referência no SuSE: SUSE-SA:2004:044

## Acrobat

O Adobe Acrobat Reader permite ler, distribuir e imprimir documentos gerados no padrão *Portable Document Format* (PDF).

A iDEFENSE divulgou uma falha no Adobe Acrobat Reader versão 5.0.9, mais precisamente um estouro de buffer, ao decodificar mensagens de email. Um invasor poderia criar um PDF malicioso, executando código arbitrário no computador da vítima caso fosse aberto. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2004-1152.

Todos os usuários do Acrobat Reader são aconselhados a atualizar o programa. O Acrobat Reader versão 5.0.10 não é vulnerável a essa falha. ■

Referência no Gentoo: GLSA 200412-12 / acroread

Referência no Red Hat: RHSA-2004:674-07

## CUPS

O Common UNIX Printing System (CUPS) é um gerenciador de impressão multiplataforma. O *hpgltops* é um filtro para o CUPS que permite a impressão de arquivos HPGL. *lppasswd* é um programa usado localmente gerenciar as senhas do sistema de impressão.

O CUPS faz uso de um trecho vulnerável do código do *Xpdf* para manipular arquivos em PDF (CAN-2004-1125). Além disso, Ariel Berkman descobriu um estouro de buffer na função *ParseCommand*, presente no arquivo `hpgl-input.c` do programa *hpgltops* (CAN-2004-1267). Finalmente, Bartlomiej Sieka descobriu inúmeros problemas no programa *lppasswd*: ele ignora alguns erros de escrita (CAN-2004-1268), gera um arquivo `passwd.new` no lugar (CAN-2004-1269) e não verifica se o arquivo `passwd.new` é diferente da saída padrão de erros STDERR (CAN-2004-1270).

As vulnerabilidades no *Xpdf* e no *hpgltops* podem ser exploradas por um agressor remoto para executar código arbitrário. Para isso, basta enviar pedidos de impressão (*jobs*) especialmente preparados para um servidor CUPS. As vulnerabilidades no *lppasswd* podem ser exploradas por um invasor local para escrever dados no arquivo de senhas do CUPS ou impedir futuras modificações nele.

Não há solução conhecida (mesmo provisória) até o presente momento. Mesmo assim, todos os usuários do CUPS devem atualizar o programa. ■

Referência no Debian: DSA-621-1

Referência no Gentoo: GLSA 200412-25 / CUPS

Referência no Mandrake: MDKSA-2004:164

## Mozilla/Firefox/Thunderbird

O Mozilla é um navegador web bastante popular que inclui um leitor de email e outro de notícias. Já o Mozilla Firefox e o Mozilla Thunderbird são, respectivamente, navegador e leitor de email da nova geração do projeto Mozilla.

Maurycy Prodeus, da isec.pl, encontrou um estouro de buffer potencialmente explorável na manipulação de URLs NNTP. Além disso, Martin (da ptraced.net) descobriu que arquivos temporários em versões recentes dos produtos Mozilla são gravados com permissões de leitura e escrita para todos os usuários e possuem nomes extremamente previsíveis. A equipe de desenvolvimento do Mozilla também tapou um buraco que permitia forjar nomes de arquivos na caixa de diálogo *What should Firefox do with this file* ("O que o Firefox deve fazer com este arquivo?") e um potencial vazamento de informações sobre a existência de arquivos locais (e seus nomes).

Um agressor remoto poderia preparar um link NNTP malicioso e persuadir o usuário a clicar nele. Resultado: execução de código arbitrário com os direitos do usuário usando o browser – que, num descuido do operador da máquina, pode ser o próprio *root*! Um agressor local pode se aproveitar da vulnerabilidade nos arquivos temporários para ler o conteúdo dos downloads e anexos de outros usuários. Um invasor remoto pode, ainda, criar uma página web maliciosa que permitiria forjar nomes de arquivo caso o usuário use a função *Open with...* (Abrir com...) no Firefox. No mínimo, será possível fazer testes para verificar a existência de arquivos específicos no sistema de arquivos local.

Não há solução conhecida (mesmo provisória) até o presente momento. Ainda assim, todos os usuários do Mozilla devem atualizar o programa para a versão mais nova. ■