Dicas de [In]segurança

Kernel

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

Foi descoberta uma falha provocada por falta de serialização na função *unix_dgram_recvmsg*, afetando kernels anteriores à versão 2.4.28. Um usuário local poderia potencialmente fazer uso de uma condição de disputa (race condition) para conseguir mais privilégios. O projeto "Common Vulnerabilities and Exposures" (cve.mitre.org) deu a essa falha o código CAN-2004-1068.

Paul Starzetz do iSEC descobriu inúmeras falhas no carregador de binários ELF afetando kernels anteriores à versão 2.4.28. Um usuário local poderia usar essas falhas para conseguir acesso a binários que tenham apenas permissão de execução ou possivelmente ganhar mais privilégios. (CAN-2004-1070, CAN-2004-1071, CAN-2004-1072, CAN-2004-1073)

Foi descoberta uma falha na definição de limites para TSS que afeta os kernels das arquiteturas AMD, AMD64 e Intel EM64T anteriores à versão 2.4.23. Um usuário local poderia usar essa falha para causar uma negação de serviço (travamento do programa) ou possivelmente ganhar mais privilégios. (CAN-2004-0812)

Foi descoberta uma falha de estouro de inteiros na função *ubsec_keysetup* do driver Broadcom 5820 cryptonet. Em sistemas usando esse driver, um usuário local poderia causar uma negação de serviço (travamento do programa) ou possivelmente ganhar privilégios de administrador do sistema. (CAN-2004-0619)

Stefan Esser descobriu inúmeras falhas incluindo estouros de pilha no driver smbfs, afetando kernels anteriores à versão 2.4.28. Um usuário local poderia causar uma negação de serviço (travamento do programa) ou possivelmente ganhar mais privilégios. Para poder explorar essas falhas o usuário precisa ter controle sobre um servidor Samba conectado à rede. (CAN-2004-0883, CAN-2004-0949)

A SGI descobriu uma falha no carregador ELF que afeta kernels anteriores à versão 2.4.25. A falha pode ser explorada por um binário (executável) mal formado. Em arquiteturas diferentes da x86, um usuário local poderia criar um binário malévolo que causaria uma negação de serviço (travamento do programa). (CAN-2004-0136)

A Conectiva descobriu diversas falhas em certos drivers USB afetando kernels anteriores à versão 2.4.27. Os drivers vulneráveis usam a função *copy_to_user* em estruturas não inicializadas. Essas falhas poderiam permitir que usuários locais tivessem acesso a pequenas porções da memória usada pelo kernel. (CAN-2004-0685)

Referência no Red Hat: RHSA-2004:549-10
Referência no SuSE: SUSE-SA:2004:042

Cyrus-imapd

O servidor Cyrus IMAP é um eficiente servidor de emails IMAP, altamente escalável. Múltiplas vulnerabilidades

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.suse.de/uk/private/support/security/* Lista: *http://www.suse.de/uk/private/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.

foram encontradas nos interpretadores de argumentos dos comandos *partial* e *fetch* do Cyrus IMAP Server (CAN-2004-1012, CAN-2004-1013). Há ainda estouros de buffer no código do 'imap magic plus' que também podem ser explorados. (CAN-2004-1011, CAN-2004-1015).

Um invasor poderia explorar essas vulnerabilidades para executar código arbitrário com os direitos do usuário no qual o Cyrus IMAP Server roda. Não há solução conhecida (mesmo provisória) até o presente momento. Todos os usuários do Cyrus-IMAP Server devem atualizar o programa para a versão mais nova. ■

Referência no Debian: DSA-597-1 cyrus-imapd
Referência no Gentoo: GLSA 200411-34 / cyrus-imapd
Referência no SuSE: SUSE-SA:2004:043

■ Sun Java Plugin

A segurança do plug-in Java fornecido pela Sun e Blackdown.org pode ser contornada, permitindo acesso a pacotes arbitrários. Isso permitiria que applets Java não autorizados executassem ações sem restrição no sistema. O projeto "Common Vulnerabilities and Exposures" (cve.mitre.org) deu a essa falha o código CVE CAN-2004-1029.

A Sun e a Blackdown oferecem, cada uma, sua implementação de kits de desenvolvimento em java (Java Development Kits – JDK) e máquinas virtuais para execução de programas compilados em Java (Java Runtime Environments – JRE). Todas essas implementações possuem um plug-in que pode ser usado para executar applets Java em ambientes restritos – especialmente navegadores. Todos os plug-ins Java estão sujeitos a uma vulnerabilidade que permite acesso irrestrito a qualquer outro pacote Java.

Um invasor remoto poderia embutir um applet Java malicioso e convencer a vítima a executá-lo. O applet pode, então, contornar as restrições de segurança e executar qualquer comando ou acessar qualquer arquivo ou diretório legível pelo usuário usando o navegador.

Como paliativo, desative a execução de applets Java em seu navegador. Todos os usuários do Sun JDK devem atualizar o programa para a versão mais nova. ■

Referência no Gentoo: GLSA 200411-38 / Java

■ Samba

O Samba é uma implementação livre e gratuita de servidores de arquivos baseados nos protocolos SMB/CIFS, permitindo interoperabilidade com serviços de impressão e compartilhamento de arquivos de outros clientes SMB/CIFS – por exemplo, sistemas operacionais Windows®. Foram identificadas diversas vulnerabilidades no Samba.

Há um problema no daemon de compartilhamento de arquivos do Samba, permitindo que um usuário remoto consuma uma quantidade impressionante de recursos e potencialmente possa derrubar o serviço se usar nomes de arquivo com coringas ("*" e "?").

Para que o ataque seja um sucesso, basta que o daemon do Samba esteja rodando e um usuário remoto tenha acesso a um compartilhamento qualquer (mesmo que apenas de leitura). O projeto "Common Vulnerabilities and Exposures" (cve.mitre.org) deu a essa falha o código CAN-2004-0930.

Stefan Esser encontrou um problema na manipulação de cadeias de caracteres Unicode do gerenciador de arquivos do Samba que leva a um estouro de buffer baseado no segmento de dados (heap) que pode ser provocado remotamente, permitindo que atacantes remotos injetem código no processo smbd. O projeto "Common Vulnerabilities and Exposures" (cve.mitre.org) deu a essa falha o código CAN-2004-0882.

Todos os usuários do Samba devem atualizar o programa para a versão indicada, que contém patches de segurança trazidos de versões mais recentes que não são vulneráveis a esses incidentes. ■

Referência no Gentoo: GLSA 200411-21 / samba
Referência no Mandrake: MDKSA-2004:136
Referência no Red Hat: RHSA-2004:632-17
Referência no SuSE: SUSE-SA:2004:040

■ Apache

O Apache é um dos servidores web (HTTP) mais populares da Internet.

Chintan Trivedi descobriu uma vulnerabilidade no Apache httpd 2.0 causada por uma limitação no comprimento de campos de dados. Essa imposição está presente no código que interpreta o cabeçalho HTTP. Ao enviar uma grande quantidade de requisições *HTTP GET*, um atacante remoto pode causar uma negação de serviço no sistema alvo. O projeto "Common Vulnerabilities and Exposures" (cve.mitre.org) deu a essa falha o código CAN-2004-0942.

"Crazy Einstein" descobriu uma vulnerabilidade no módulo *mod_include* que pode causar um estouro de buffer e levar à execução de código arbitrário. O projeto "Common Vulnerabilities and Exposures" (cve.mitre.org) deu a essa falha o código CAN-2004-0940.

Larry Cashdollar descobriu um estouro de pilha em potencial no utilitário *htpasswd* que pode ser explorado quando dados do usuário são passados a ele através de um CGI (ou PHP ou Perl...). Todos os usuários do Apache devem atualizá-lo para a versão mais nova. ■

Referência no Debian: DSA-594-1 apache
Referência no Gentoo: GLSA 200411-18 / apache
Referência no Mandrake: MDKSA-2004:134
Referência no Red Hat: RHSA-2004:562-11

sudo

O *sudo* é um programa que concede poderes limitados de superusuário a usuários específicos. Liam Helmer descobriu, entretanto, que o *sudo* não "limpa" o ambiente como deveria. Funções do shell Bash e a variável de ambiente *CDPATH* ainda são repassados para o programa rodando com permissões privilegiadas, permitindo que rotinas do sistema sejam sobrecarregadas. O projeto "Common Vulnerabilities and Exposures" (cve.mitre.org) deu a essa falha o código CAN-2004-1051.

Essas vulnerabilidades só podem ser exploradas por usuários que estão cadastrados no arquivo sudoers e, portanto, possuem privilégios limitados de superusuário. Recomendamos que o pacote sudo seja atualizado o mais rápido possível. ■

Referência no Debian: DSA-596-2 sudo
Referência no Mandrake: MDKSA-2004:133

Ruby

Ruby é uma linguagem interpretada para scripts que permite desenvolvimento rápido e orientado a objetos. O módulo de CGI do Ruby pode ser usado para construir sistemas web.

Os desenvolvedores do Ruby encontraram um problema no módulo de CGI que pode ser disparado remotamente e que causa um laço de execução (loop) infinito. Um atacante remoto poderia disparar a vulnerabilidade através de um sistema web em Ruby que esteja vulnerável e causar o uso desnecessário de tempo de CPU por parte do servidor. Um certo número desses loops rodando simultaneamente pode provocar uma negação de serviço por esgotamento de recursos. O projeto "Common Vulnerabilities and Exposures" deu a essa falha o código CAN-2004-0983.

Não há solução conhecida até o presente momento. Todos os usuários do Ruby até a versão 1.6.x devem atualizar o programa para a versão mais nova. ■

Referência no Mandrake: MDKSA-2004:128

Openssl e Groff

O OpenSSL é um subsistema que implementa os protocolos SSL (Secure Socket Layer) e TLS (Transport Layer Security), bem como uma biblioteca de criptografia para uso geral. Inclui também o script *der_chop* para converter certificados codificados no padrão DER para o formato PEM. O Groff (GNU Troff) é um pacote de formatação de textos que lê arquivos de texto contendo comandos de formatação e produz um documento formatado. No pacote há o comando *groffer*, que mostra arquivos groff e páginas de manual (man pages) no X e no console (tty).

Tanto o *groffer* quanto o *der_chop* criam arquivos temporários nos diretórios em que as permissões sejam as mais universais possíveis (como o /tmp, por exemplo). Esses arquivos possuem nomes fáceis de prever. Um usuário local malicioso poderia criar links simbólicos no diretório temporário que apontem para um arquivo válido em outra parte do sistema de arquivos. Como resultado, rodar os scripts *groffer* e *der_chop* pode sobrescrever os arquivos para os quais os links apontam. Como é possível (e bem provável) que o próprio root execute esses scripts, nenhum arquivo do sistema está a salvo. Potencialmente, é possível comprometer de forma severa toda a segurança do sistema. Para mais informações sobre esse problema, consulte os documentos CVE CAN-2004-0969 e CAN-2004-0975 do Mitre

Não há solução conhecida (mesmo provisória) até o presente momento. ■

Referência no Debian: DSA-603-1 openssl
Referência no Gentoo: GLSA 200411-15 / OpenSSL
Referência no Mandrake: MDKSA-2004:147

BNC

O BNC é um proxy que "ricocheteia" sessões IRC. Leon Juranic descobriu que o BNC nem sempre protege os buffers, evitando que sejam estourados. Um servidor IRC malicioso poderia explorar a falha e fazer o limitado buffer transbordar, permitindo a execução de código arbitrário. O projeto "Common Vulnerabilities and Exposures" (cve.mitre.org) deu a essa falha o código CAN-2004-1052. ■

Referência no Debian: DSA-595-1 bnc
Referência no Gentoo: GLSA 200411-24 / BNC

ez-ipupdate

O ez-ipupdate é um utilitário para a atualização de informações de nome de hosts para serviços de DNS. Ulf Harnhammar, do Debian Security Audit Project, descobriu uma vulnerabilidade de formatação em cadeias de caracteres no ez-ipupdate. Um invasor poderia explorar a falha para executar código arbitrário com as permissões do usuário rodando o ez-ipupdate, que poderia ser o próprio root. O projeto "Common Vulnerabilities and Exposures" deu a essa falha o código CAN-2004-0980.

Não há solução conhecida até o presente momento. Mesmo assim, todos os usuários do ez-ipupdate são aconselhados atualizar o programa para a versão mais nova. ■

Referência no Debian: DSA-592-1 ez-ipupdate
Referência no Gentoo: GLSA 200411-20 / ez-ipupdate

Sergio Ianni: www.sxc.hu