Dicas de (In)Segurança

Subversion

O Subversion é um sistema de controle de versão similar ao popular CVS.

O código do subversion é vulnerável a um estouro de buffer na pilha que pode ser remotamente explorado. Este erro acontece antes de qualquer processo de autenticação. Um agressor pode usar esta vulnerabilidade para executar um código qualquer.

O projeto "Common Vulnerabilities and Exposures" deu a este problema o código CAN-2004-0413.

Código de Referência no Suse: SuSE-SA:2004:018
Código de Referência no Gentoo: GLSA 200406-07 / Subversion

Kernel

Recentemente foram descobertas múltiplas vulnerabilidades de segurança no kernel do Linux.

Uma falha nas versões 2.4 e 2.6 do kernel para as arquiteturas x86 e x86_64 permite que usuários locais causem uma negação de serviço (derrubem o sistema) ao ativar um receptor de sinal com uma certa seqüência de instruções fsave e fstor. O projeto "Common Vulnerabilities and Exposures" deu a este problema o código CAN-2004-0554.

Outra falha foi descoberta na chamada de sistema clone(). Ela permite que usuários locais causem uma negação de serviço (vazamento de memória) ao passar argumentos inválidos para clone() dentro de um loop infinito em um programa. O projeto "Common Vulnerabilities and Exposures" deu a este problema o código CAN-2004-0427.

Al Viro fez melhorias no kernel 2.6 que permitem que a ferramenta de checagem de código esparso procure por certos tipos de bugs no kernel. Vulnerabilidades no acesso à memória do kernel nos drivers e1000, decnet, acpi_asus, alsa, aito/WLAN, pss e mpu401 foram corrigidas. Estas vulnerabilidades podem levar à leitura e escrita da memória do kernel e negação de serviço local, resultando na possibilidade de um agressor com uma conta local ter acesso à conta de root do sistema. O projeto "Common Vulnerabilities and Exposures" deu a este problema o código CAN-2004-0495.

Um vazamento de informações que afeta apenas os sistemas ia64 também foi descoberto. O projeto "Common Vulnerabilities and Exposures" deu a este problema o código CAN-2004-0565.

Código de Referência no Mandrake: MDKSA-2004:066
Código de Referência no Red Hat: RHSA-2004:255-10

DHCP

O servidor DHCP (Dynamic Host Configuration Protocol) é usado para configurar dinamicamente clientes que se conectam a uma rede ("hotspots" wireless, redes empresariais, etc...)

Uma vulnerabilidade no modo como o servidor DHCPD do ISC (Internet Systems Consortium) lida com o registro das atividades do servidor via syslog pode permitir que um agressor derrube o daemon e cause um ataque de negação de serviço (Denial of Service - DOS) ao enviar pacotes especiais para a porta de escuta do DHCPD. Existe a possibilidade de execução de código com as permissões do usuário que está rodando o servidor, geralmente o root. A United States Computer Emergency Readiness Team (U.S. CERT) deu a este problema o código VU#317350.

Existe uma vulnerabilidade similar no modo como o DHCPD do ISC usa a função vsnprintf() em um sistema que não a suporta. Esta vulnerabilidade também pode ser usada para execução de código e/ou um ataque de negação de serviço. As declarações da função vsnprintf() afetadas estão logo depois do código mencionado no parágrafo anterior. A United States Computer Emergency Readiness Team (U.S. CERT) deu a este problema o código VU#654390.

Código de Referência no Suse: SuSE-SA:2004:019
Código de Referência no Mandrake: MDKSA-2004:061

SquirrelMail

O SquirrelMail é um sistema de webmail escrito em PHP. Foram encontradas múltiplas vulnerabilidades em uma das versões do software.

Uma falha que permite a injeção de comandos SQL foi encontrada no SquirrelMail 1.4.2 e versões anteriores. Se o SquirrelMail estiver configurado para armazenar o livro de endereços do usuário na base de dados, um agressor remoto pode usar esta falha para executar comandos SQL. O projeto "Common Vulnerabilities and Exposures" deu a esta falha o código CAN-2004-0521.

Também foram encontradas várias falhas no recurso "cross-site scripting" (XSS) no SquirrelMail 1.4.2 e versões anteriores, que permitem a um agressor remoto executar um script com os privilégios de outro usuário. O projeto "Common Vulnerabilities and Exposures" deu a este problema os códigos CAN-2004-0519 e CAN-2004-0520.

Código de Referência no Red Hat: RHSA-2004:240-06
Código de Referência no Gentoo: GLSA 200405-16 / SquirrelMail

Sup

O Sup (*Systems Utility Page*) é um aplicativo modular, escrito em PHP, que pode ser usado para monitorar e executar comandos em servidores locais ou remotos, além de sincronizar repositórios de arquivos. Pode ser encontrado no endereço: *http://freshmeat.net/projects/sup/*.

O usuário *jaguar@felinemenace.org* encontrou uma vulnerabilidade no sup que possibilita a um agressor remoto a execução de código com os mesmos privilégios de acesso do proprietário do processo *sup-filesrv*.

O problema está em uma string de formatação do syslog(3), encontrada nas funções logquit, logerr e loginfo. O projeto "Common Vulnerabilites and Exposures" deu a esta falha o código CAN-2004-0451.

Código de Referência no Debian: DSA-521-1 sup — format string vulnerability

Libpng

O pacote libpng contém uma biblioteca com funções para criar e manipular imagens no formato PNG (Portable Network Graphics), uma alternativa livre ao popular formato GIF.

Durante uma auditoria nas atualizações da Red Hat, a equipe Fedora Legacy encontrou uma falha de segurança na biblioteca libpng que não havia sido corrigida no Red Hat Enterprise Linux 3. Um agressor pode criar um arquivo PNG que causa a queda de um aplicativo ligado à libpng, com a possibilidade de execução de código quando a imagem é aberta.

Foi descoberto um estouro de buffer causado pelo cálculo incorreto do valor de offset de um loop. Esta falha pode levar a um ataque de negação de serviço (DoS) ou mesmo comprometimento remoto do sistema.

Esta vulnerabilidade foi originalmente corrigida em janeiro de 2003, mas desde então descobriu-se que dois outros pontos do código também afetados não foram corrigidos. O projeto "Common Vulnerabilities and Exposures" deu a este problema o código CAN-2002-1363.

Código de Referência no Mandrake: MDKSA-2004:063
Código de Referência no Red Hat: RHSA-2004:249-07
Código de Referência no Gentoo: GLSA 200407-06 / libpng

Apache

O servidor HTTP Apache é um servidor web completo, poderoso, eficiente e livremente disponível na Internet.

Um vazamento de memória que pode ser causado remotamente foi descoberto na versão 2.0.50 do servidor HTTP Apache. Isto possibilita que um agressor remoto cause um ataque de negação de serviço (DoS) ao fazer o servidor web consumir grandes quantidades de memória. O projeto "Common Vulnerabilities and Exposures" deu a esta falha o código CAN-2004-0493.

George Guninski descobriu uma outra falha que pode levar a um ataque de negação de serviço (DoS) no Apache 2.x. Esta falha também pode fazer com que o servidor web consuma mais memória que o normal. Em sistemas de 64 Bits com mais de 4 GB de memória virtual, ainda raros, isto também pode levar a um estouro da pilha.

Um estouro de buffer também foi encontrado por George Gudinski no módulo mod_proxy do Apache. Esta falha pode ser explorada por um usuário remoto para potencialmente executar código com os privilégios de acesso do proprietário do processo-filho do httpd (geralmente o usuário apache ou www-data). Contudo, esta falha só pode ser explorada se o módulo mod_proxy realmente estiver em uso.

Note que este bug existe em um módulo no pacote apache-common, compartilhado pelo apache, apache-ssl e apache-perl, de forma que uma única atualização é suficiente para corrigir estas três variantes do servidor httpd. Contudo, em sistemas usando o apache-ssl ou apache-perl, o daemon httpd não será reinicializado automaticamente. O projeto "Common Vulnerabilities and Exposures" deu a este problema o código CAN-2004-0492.

Código de Referência no Mandrake: MDKSA-2004:064 e MDKSA-2004:065
Código de Referência no Red Hat: RHSA-2004:342-10
Código de Referência no Debian: DSA-525-1 apache — buffer overflow
Código de Referência no Gentoo: GLSA 200407-03 / Apache

Super

O Super é um programa que permite a usuários específicos executar comandos com privilégios de root, de forma similar ao sudo. Pode ser encontrado no endereço *http://freshmeat.net/projects/super/*.

Max Vozeler descobriu uma vulnerabilidade em uma string de formatação no super. Esta vulnerabilidade pode ser explorada por um usuário local para executar código com privilégio de root.

O projeto "Common Vulnerabilities and Exposures" deu a este problema o código CAN-2004-0579.

Código de Referência no Debian: DSA-522-1 super — format string vulnerability

www-sql

O www-sql é um programa que permite a criação de páginas HTML dinâmicas através da inclusão de tags especiais, possibilitando a interação com bancos de dados SQL, como o PostGreSQL.

Ulf Härnhammar descobriu um buffer overflow no módulo www-sql. Ao explorar esta vulnerabilidade, um usuário local pode executar código ao criar e processar uma página com o www-sql.

O projeto "Common Vulnerabilities and Exposures" deu a este problema o código CAN-2004-0455.

Código de Referência no Debian: DSA-523-1 www-sql — buffer overflow

rlpr

O rlpr é um pacote que permite a sistemas remotos imprimir arquivos em uma impressora local.

O usuário *jaguar@felinemenace.org* descobriu uma vulnerabilidade em uma string de formatação no rlpr. Ao investigar esta falha, um buffer overflow foi descoberto em um trecho de código relacionado. Ao explorar estas vulnerabilidades, um usuário local ou remoto pode causar execução de código com os privilégios do proprietário do processo rlprd (no caso de um usuário remoto) ou root (no caso de um usuário local).

O primeiro erro é uma vulnerabilidade em uma string de formatação do syslog(3) na função msg() no rlpr. O projeto "Common Vulnerabilities and Exposures" deu a este problema o código CAN-2004-0393.

O outro problema é um buffer overflow também na função msg() no rlpr. O projeto "Common Vulnerabilities and Exposures" deu a este problema o código CAN-2004-0454.

Código de Referência no Debian: DSA-524-1 rlpr — several vulnerabilities

Pavuk

Pavuk é um aplicativo usado para espelhar websites ou arquivos. Ele pode transferir documentos de servidores HTTP, FTP, Gopher e opcionalmente HTTPS (HTTP sobre SSL). O software pode ser encontrado no endereço *http://www.idata.sk/~ondrej/pavuk/*

Ulf Härnhammar descobriu uma vulnerabilidade no Pavuk, no qual uma resposta HTTP 305 grande demais enviada por um servidor malicioso pode possibilitar a execução de código com os privilégios do proprietário do processo pavuk.

O projeto "Common Vulnerabilities and Exposures" deu a este problema o código CAN-2004-0456.

Código de Referência no Debian: DSA-527-1 pavuk — buffer overflow
Código de Referência no Gentoo: GLSA 200406-22 / Pavuk