Dicas de (In)Segurança

Tripwire

Tripwire é uma ferramenta que procura por mudanças em seu sistema. O programa monitora atributos chave de arquivos que não devem mudar, incluindo assinatura binária, tamanho, mudanças esperadas de tamanho, etc. Conhecida como uma ferramenta para detecção de intrusão, pode ser usada para muitos outros fins, como verificação de integridade, gerenciamento de mudanças e muito mais.

Paul Herman descobriu uma vulnerabilidade relativa à uma string de formatação no programa. Isso permite que um usuário local execute um código qualquer com as permissões do usuário que está executando o tripwire (tipicamente root). Esta vulnerabilidade existe apenas quando o Tripwire está gerando um e-mail de relatório.

O projeto "Common Vulnerabilities and Exposures" deu a este problema o código CAN-2004-0536. ■

Código de Referência do Mandrake: MDKSA-2004:057

xpcd

O xpcd é um visualizador de PhotoCD. Ele lê um arquivo com thumbnails e permite que você navegue pelas imagens. Uma vulnerabilidade no xpcd-svga, incluso no pacote xpcd, foi descoberta por Jaguar. xpcd-svga usa a svgalib para mostrar imagens no console, e pode copiar dados de tamanho arbitrário fornecidos pelo usuário em um buffer de tamanho fixo na função pcd_open. Além disso, Steve Kemp descobriu um outro buffer overflow no xpcd-svga que poderia ser causado pelo uso de uma variável $HOME muito longa. Isto poderia ser explorado por um agressor local para obter privilégio de root no sistema.

O projeto "Common Vulnerabilities and Exposures" deu estes problemas deu os códigos CAN-2004-0649 e CAN-2004-0402, respectivamente. ■

Código de Referência do Mandrake: MDKSA-2004:053
Código de Referência do Debian: DSA-508-1 xpcd – buffer overflow

Servidor Kolab

Luca Villani reportou a divulgação de informações críticas de configuração no servidor Kolab, parte do projeto KDE Groupware. As versões afetadas armazenam senhas OpenLDAP em texto puro. O coração do Kolab é um sistema escrito em Perl que reescreve os arquivos de configuração de certos aplicativos com base em templates. A função build() deixava o arquivo slapd.conf com permissão global para leitura, exibindo a senha de root do OpenLDAP. ■

Código de Referência do Mandrake: MDKSA-2004:052

mod_ssl

Há um buffer overflow no gerenciamento de pilha da função ssl_util_uuencode_binary, que faz parte do arquivo ssl_engine_kernel.c, nas versões do mod_ssl para o servidor web Apache 1.3.x. Quando o mod_ssl é configurado para confiar na autoridade de certificação, um agressor remoto pode executar código arbitrário através de um certificado do cliente com um campo assunto (DN) longo.

O projeto "Common Vulnerabilities and Exposures" deu a este problema o código CAN-2004-0488. ■

Código de Referência do Mandrake: MDKSA-2004:054

Postura das Principais Distribuições quanto à Segurança

Distribuição	Referência de Segurança	Comentários
Conectiva	Info: *http://distro2.conectiva.com.br/seguranca/* Lista: *seguranca-admin@distro.conectiva.com.br* e *http://distro2.conectiva.com.br/lista/* Referência: CLSA-...[1]	Possui uma página específica sobre segurança, mas não há link para ela na página principal. Os alertas são distribuídos através de e-mails assinados com a chave PGP da empresa, para assegurar sua autenticidade, e contém 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 com o 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/* Patches: *http://www.suse.de/uk/private/download/updates/* Lista: 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 mostrado 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.

LHA

LHA é um utilitário para arquivamento e compressão de dados no formato LHarc. Ulf Harnhammar encontrou um buffer overflow na pilha e falhas no tratamento de diretórios.

Um agressor pode explorar os múltiplos buffer overflows na pilha, que ocorrem na função get_header no arquivo header.c do LHA 1.14, se criar um arquivo LHA cuidadosamente estruturado de forma que o código seja executado quando o arquivo é testado ou descompactado pela vítima. O projeto "Common Vulnerabilities and Exposures" deu a este problema o código CAN-2004-0234.

Um agressor pode explorar as múltiplas falhas no tratamento de diretórios no LHA 1.14 para possibilitar que agressores remotos, ou usuários locais, criem arquivos arbitrários usando arquivos LHA com (1) sequências fazendo referência a .. e (2) caminhos absolutos com barras duplas ("//caminho/absoluto").

O projeto "Common Vulnerabilities and Exposures" deu a este problema o código CAN-2004-0235.

Código de Referência do Red Hat: RHSA-2004:178-09
Código de Referência do Debian: DSA-515-1 lha – several vulnerabilities

Krb5

O Kerberos é um sistema de autenticação em rede. Bugs foram encontrados na função krb5_aname_to_localname da biblioteca. Mais especificamente, buffer overflows são possíveis em todas as versões do Kerberos até a 1.3.3 (inclusive).

A função citada traduz um nome principal Kerberos para um nome de uma conta local, tipicamente um nome de usuário UNIX. Ela é freqüentemente usada na verificação de autorizações.

Se configuradas para mapear nomes principais Kerberos específicos para determinados nomes de usuário UNIX, certas funções chamadas por krb5_aname_to_localname não irão verificar o tamanho dos buffers usados para armazenar partes do nome principal. Se configurado para mapear principais para nomes de usuários usando regras, krb5_aname_to_localname consistentemente escreve um byte além do fim do buffer alocado a partir da pilha.

Somente configurações que habilitem o mapeamento explícito ou baseado em regras que krb5_aname_to_localname() retorna são vulneráveis a esse problema. Essa configuração não é feita por padrão.

O projeto "Common Vulnerabilities and Exposures" deu a este problema o número CAN-2004-0523.

Código de Referência do Mandrake: MDKSA-2004:056-1
Código de Referência do Red Hat: RHSA-2004:236-14

Ethereal

O Ethereal é um programa para monitorar e analizar tráfego de rede. O separador MMSE nas versões 0.10.1 a 0.10.3 contém um buffer overflow. Em um sistema que esteja executando o Ethereal, um agressor remoto pode enviar pacotes maliciosos que fazem com que o Ethereal caia ou execute código arbitrário. Além disso, outras falhas em versões do Ethereal anteriores à 0.10.4 foram encontradas, que fazem com que o programa caia em resposta à pacotes SIP, AIM ou SPNEGO especialmente construídos.

O projeto "Common Vulnerabilities and Exposures" deu a estas falhas os códigos CAN-2004-0507, CAN-2004-0504, CAN-2004-0505 e CAN-2004-0506.

Código de Referência do Red Hat: RHSA-2004:234-06
Código de Referência do Debian: DSA-511-1 ethereal – buffer overflows

CVS

O Concurrent Versions System (CVS) oferece ferramentas que permitem aos desenvolvedores compartilhar e manter grandes projetos de software e é freqüentemente usado para para manter repositórios de código-fonte.

Enquanto investigava uma vulnerabilidade anterior, já corrigida, Derek Price descobriu uma falha relativa a linhas "Entry" mal-formadas que levam à falta de um terminador nulo na string. O projeto "Common Vulnerabilities and Exposures" deu a esta falha o código CAN-2004-0414.

Stefan Esser e Sebastian Krahmer conduziram uma auditoria no CVS e corrigiram uma série que problemas que poderiam levar a falhas de segurança. Entre os itens considerados passíveis de exploração estavam:

- Uma condição double-free relacionada à string error_prog_name.
- Ao enviar um grande número de argumentos ao servidor CVS, é possível fazê-lo alocar uma grande quantidade de memória, que não cabe no espaço de endereçamento, causando um erro.
- Escritas fora dos limites na função serv_notify()

Um agressor com acesso a um servidor CVS pode ser capaz de executar código arbitrário sob o UID que estiver executando o servidor CVS.

O projeto "Common Vulnerabilities and Exposures" deu a estas falhas os códigos CAN-2004-0416, CAN-2004-0417 e CAN-2004-0418.

Código de Referência do SuSE: SuSE-SA:2004:015
Código de Referência do Mandrake: MDKSA-2004:058
Código de Referência do Red Hat: RHSA-2004:233-07
Código de Referência do Debian: DSA-517-1 cvs – buffer overflow

KDElibs

O pacote kdelibs3 é um dos pacotes base para o K Desktop Environment, ou KDE. O manipulador de URIs da biblioteca de classes do kdelibs e kdelibs3 contém uma falha que permite que atacantes remotos criem arquivos com as permissões do usuário que está executando o pacote kdelibs/kdelibs3. Isto afeta aplicativos que utilizam o tal manipulador, como Konqueror e KMail.

O projeto "Common Vulnerabilities and Exposures" deu a esta falha o código CAN-2004-0411.

Código de Referência do SuSE: SuSE-SA:2003:014

Squid

O Squid é um web proxy/cache. O aplicativo auxiliar usado para autenticação NTLM no Squid é vulnerável a um buffer overflow que pode ser explorado remotamente com o envio de uma senha longa demais, o que leva a um estouro do buffer, possibilitando a execução de código arbitrário. Se o Squid for configurado para trabalhar com autenticação NTLM, essa falha pode ser explorada.

O projeto "Common Vulnerabilities and Exposures" deu a esta falha no Squid código CAN-2004-0541.

Código de Referência do SuSE: SuSE-SA:2004:016
Código de Referência do Mandrake: MDKSA-2004:059
Código de Referência do Red Hat: RHSA-2004:242-06

Gallery

Um bug foi descoberto no Gallery, um álbum de imagens escrito em PHP. Graças a este bug, um agressor pode conseguir acesso ao usuário "admin" da galeria, sem a necessidade de autenticação.

O projeto "Common Vulnerabilities and Exposures" deu a esta falha o código CAN-2004-0522. O projeto Debian lançou uma atualização para o software

Código de Referência do Debian: DSA-512-1 gallery – unauthenticated access

Gatos

Steve Kemp descobriu uma falha no xatitv, um dos programas do pacote gatos, usado para exibir vídeo em certas placas de vídeo da ATI.

xativ é instalado com setuid root para ganhar acesso direto ao hardware de vídeo. Normalmente o aplicativo abandona o privilégio de root logo após a inicialização. Contudo, se a inicialização falhar devido à falta de um arquivo de configuração, os privilégios não são abandonados, e o xatitv usa a função system (3) para executar seu aplicativo de configuração sem limpar variáveis de ambiente fornecidas pelo usuário.

Ao explorar esta vulnerabilidade, um agressor pode conseguir privilégios de root caso o arquivo de configuração não exista. Contudo, um arquivo de configuração padrão é fornecido no pacote, portanto esta falha não pode ser explorada a não ser que o arquivo de configuração seja removido pelo administrador.

O projeto "Common Vulnerabilities and Exposures" deu a esta falha o código CAN-2004-0395.

Código de Referência do Debian: DSA-509-1 gatos – privilege escalation

Linux Kernel I

Adam Osuchowski e Tomasz Dubinski descobriram uma falha de segurança grave no código do iptables que acompanha o Linux Kernel 2.6. O problema é que um tipo incorreto foi utilizado para uma variável da função tcp_find_option(). Quando iptables é configurado com opções TCP (--tcp-option), agressores remotos podem levar o Kernel a parar utilizando pacotes TCP especialmente preparados. Um sistema assim atacado torna-se inacessível via rede.

Osuchowski e Dubinski fornecem a descrição e uma correção (patch) para o problema em um Advisory no arquivo BugTraq. A correção consiste em modificar o tipo da variável "opt", que está definida como uma array de signed char, no tipo unsigned char ou U_int8_t, que é como ela está declarada na mesma função do Kernel 2.4.

Código de Referência do SuSE: SuSE-SA:2004:020

Linux Kernel II

Durante uma auditoria de segurança no Kernel do Linux, Michael Schröder e Rüdiger Örtel, ambos da empresa SuSE, descobriram um problema de segurança, que, sob certas circunstâncias, permite a usuários comuns realizarem modificações não autorizadas no group ID de qualquer arquivo utilizando o comando chown. O group ID define a qual grupo de usuários um arquivo pertence no sistema de arquivos. Agressores locais podem utilizar modificações no group ID no intuito de estender seus direitos de acesso até obter status de administrador do sistema (root).

O problema, que está documentado em um Security Advisory, se encontra na checagem incorreta do chamado Discretionary Access Control (DAC) na função fchown(). No entanto, esta vulnerabilidade pode somente ser explorada para arquivos que tenham sido exportados por um servidor NFS e montados localmente pelo usuário. Além disso, esta falha de segurança permite também modificar o group ID de arquivos no diretório /proc. Ainda de acordo com o Security Advisory, esta última alternativa não é possível para usuários que não disponham de status de administrador.

Tanto o Kernel 2.4 quanto o 2.6 estão comprometidos pelo problema. Tanto a SuSE quanto Red Hat e Fedora disponibilizaram pacotes com a correção para o problema (patches).

O projeto "Common Vulnerabilities and Exposures" deu a esta falha o código CAN-2004-0497.

Código de Referência do SuSE: SuSE-SA:2004:020
Código de Referência do Red Hat: RHSA-2004:354-08

PHP4/mod_php4

PHP é uma linguagem script muito popular utilizada em servidores web para oferecer conteúdo dinâmico.

Stefan Esser descobriu uma falha de segurança no código do interpretador PHP com a qual um agressor remoto poder forçá-lo a atingir o limite de memória em determinados trechos de código não preparados para esta condição, o que pode levar à execução de código arbitrário utilizando o ID do usuário rodando o interpretador.

Além disso, a função script_tags(), utilizada geralmente para validar a entrada de usuários, pode permitir tags que tivessem o caracter null. Isso possibilita a agressores remotos a execução de ataques XSS (cross-site scripting).

Conectiva e SuSE disponibilizaram pacotes de atualização para o programa que corrigem esta vulnerabilidade.

O projeto "Common Vulnerabilities and Exposures" deu a estas falhas de segurança os códigos CAN-2004-0594 e CAN-2004-595.

Código de Referência da Conectiva: CLA-2004:847
Código de Referência do SuSE: SuSE-SA:2004:021

Webmin

Keigo Yamazaki reportou uma vulnerabilidade no webmin (até a versão 1.140) que possibilita a usuários não autenticados obter acesso de leitura à configuração de um módulo. O problema pode ser sanado com a atualização do webmin para a versão 1.150, que pode ser baixada diretamente do site do projeto.

Várias distribuições disponibilizaram pacotes de atualização do webmin que resolvem o problema.

O projeto "Common Vulnerabilities and Exposures" deu a esta falha o código CAN-2004-0582.

Código de Referência da Conectiva: CLSA-2004:848
Código de Referência do Debian: DSA-526-1 webmin - several vulnerabilities
Código de Referência do Gentoo: GLSA-200406-12