Dicas de [In]segurança

CUPS

O *Common UNIX Printing System* implementa um servidor de impressão em rede para sistemas operacionais UNIX® como o Linux, BSD e Mac OS X.

Um estouro de *buffer* foi encontrado na função *Decrypt::makeFileKey2* do utilitário *Xpdf*; ele também afeta o filtro *pdftops* do CUPS devido à reutilização de código. Um invasor que possa imprimir um arquivo PDF especialmente elaborado poderia executar código arbitrário como o usuário *lp*. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2005-0064.

Recomenda-se que todos os usuários do CUPS atualizem seus sistemas, pois as correções encontradas nas versões mais recentes corrigem estas falhas. ■

Referência no Debian: DSA-645-1 cupsys
Referência no Gentoo: GLSA 200501-30 / CUPS
Referência no Mandrake: MDKSA-2005:018
Referência no Red Hat: RHSA-2005:049-08
Referência no SuSE: SUSE-SR:2005:003

Kernel Linux

O kernel Linux é o núcleo do sistema operacional e desempenha funções básicas, inicializa e gerencia o acesso ao hardware, além de fazer a "interface" entre ele e os aplicativos. Este extenso alerta inclui correções para inúmeras falhas de segurança:

- O *iSEC Security Research* descobriu uma falha na manipulação de VMA na chamada de sistema *uselib* (2) do kernel Linux. Um usuário local pode abusar dessa falha para ganhar privilégios mais altos no sistema, possivelmente de root. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2004-1235.
- Em outra falha, um binário executável pode causar uma sobreposição de VMA, levando ao travamento do sis-

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.*

tema. Um usuário local pode disparar a falha criando um binário malicioso no formato *a.out* em sistemas de 32 bits ou um binário *ELF* em sistemas baseados na arquitetura de 64 bits Itanium, da Intel. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) atribuiu a essa falha o seguinte código: CAN-2005-0003.

- Outra falha descoberta pelo *iSEC Security Research*, desta vez no código que manipula as falhas de paginação, pode permitir que usuários locais ganhem privilégios mais altos no sistema, possivelmente de root, em máquinas multiprocessadas. O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2005-0001.
- Uma falha no código de filtragem das chamadas de sistema no subsistema de auditoria pode permitir que um usuário local cause o travamento do sistema caso a auditoria seja ativada, o que pode ser classificado como uma negação de serviço (DoS). O projeto *Common Vulnerabilities and Exposures* (cve.mitre.org) deu a essa falha o código CAN-2004-1237.
- Olaf Kirch descobriu que as recentes correções de segurança para o *cmsg_len* (veja o código CAN-2004-1016) quebraram a compatibilidade com aplicativos de 32 bits executados em plataformas de 64 bits como a AMD64 e sua derivativa, a Intel EM64T. Um *patch* que corrige a falha já foi liberado.
- Um documento preliminar (*draft*, ou rascunho) para a Internet, de autoria de Fernando Gont, recomenda que mensagens ICMP do tipo *Source Quench* sejam ignoradas por qualquer computador ligado à rede mundial. Um *patch* que corrige a falha já foi liberado. ■

Referência no Mandrake: MDKSA-2005:022
Referência no Red Hat: RHSA-2005:043-13

❒ Python

Criada em 1991 por Guido van Rossum, *Python* é uma linguagem de programação interpretada, interativa e orientada a objetos. Está disponível em versões para várias plataformas, entre elas sistemas UNIX® como Linux, BSD e Mac OS X, e também sistemas Windows.

Graham Dumpleton descobriu que servidores XML-RPC que façam uso da biblioteca *SimpleXMLRPCServer* são vulneráveis a uma falha de segurança que permite ler e modificar variáveis globais do módulo associado. A falha ocorre somente se a biblioteca usar o método *register_instance()* para registrar um objeto que não possua o método *_dispatch()*.

Um invasor remoto poderia se aproveitar da falha nesses servidores XML-RPC para executar código arbitrário com as permissões do usuário que roda o daemon XML-RPC.

Os usuários do *Python* que não usem servidores XML-RPC baseados na biblioteca *SimpleXMLRPCServer*, ou que usem servidores que façam uso *apenas* do método *register_function()* não são afetados por esta falha. De qualquer forma, recomenda-se que todos os usuários de *Python* atualizem o programa para a versão mais recente. ■

Referência no Gentoo: GLSA 200502-09 / Python
Referência no Mandrake: MDKSA-2005:017

❒ Squid

O *Squid* é um *proxy* para a *web* desenvolvido para sistemas Unix. Faz *proxy* e *cache* dos protocolos HTTP e FTP, entre outros, e permite conexão seguras por SSL, *cache* hierarquizado, *cache* transparente e listas de controle de acesso (ACL – *Access Control Lists*), entre muitos outros recursos.

O *Squid* possui inúmeras vulnerabilidades, entre elas um estouro de *buffer* na função *WCCP recvfrom()* (código CAN-2005-0211), verificação inconsistente dos cabeçalhos HTTP (códigos CAN-2005-0173 e CAN-2005-0174) e interpretação errônea de contas LDAP que possuam espaços em seus nomes (código CAN-2005-0175).

Um agressor poderia explorar:

- o estouro de *buffer* no *WCCP*, o que causaria uma negação de serviço (DoS);
- as falhas de verificação do cabeçalho HTTP, injetando dados arbitrários de resposta e potencialmente levando a impostura (*spoofing*) de conteúdo, envenenamento do *cache* de páginas web e outros ataques entre sites (conhecidos como *cross-site scripting*) e divisão de resposta HTTP;
- a falha de LDAP, com uma rajada de tentativas de *login* que causariam envenenamento dos *logs*.

Recomenda-se que todos os usuários do Squid atualizem o programa para a versão mais nova. ■

Referência no Debian: DSA-667-1 squid
Referência no Gentoo: GLSA 200502-04 / squid
Referência no SuSE: SUSE-SR:2005:003