Dicas de [In]segurança

CUPS

O Common UNIX Printing System (CUPS) é um serviço de impressão.

Alvaro Martinez Echevarria relatou um bug na implementação do Internet Printing Protocol (IPP) do CUPS em versões anteriores à 1.1.21. Um atacante poderia enviar um pacote UDP cuidadosamente construído para a porta IPP, fazendo com que o CUPS parasse de ouvir a porta – o que resultaria numa negação de serviço. Para explorar esse bug, um atacante precisaria ter a capacidade de enviar um pacote UDP à porta IPP (por padrão, 631). O projeto Common Vulnerabilities and Exposures (cve.mitre.org) deu a esse problema o nome CAN-2004-0558. ■

Referência no Debian: DSA-545-1
Referência no Gentoo: GLSA 200410-06 / cups
Referência no Mandrake: MDKSA-2004:097
Referência no Red Hat: RHSA-2004:449-17
Referência no Slackware: SSA:2004-266-01
Referência no Suse: SUSE-SA:2004:031

XFree86

O XFree86 é uma implementação de código aberto do sistema X Window. Traz a funcionalidade básica de baixo nível sobre a qual funcionam interfaces com o usuário (GUIs) emperiquitadas como o GNOME e o KDE.

Durante uma auditoria no código fonte, Chris Evans descobriu diversas falhas de estouro de pilha (buffer overflow) e uma falha de sobrecarga de inteiros na biblioteca X.Org *libXpm*, usada para decodificar imagens XPM (X PixMap). Um atacante poderia criar um arquivo XPM que derrubaria o aplicativo ou executaria um código arbitrário, caso fosse aberto por uma vítima. O projeto Common Vulnerabilities and Exposures (cve.mitre.org) deu a esses problemas os nomes CAN-2004-0687, CAN-2004-0688 e CAN-2004-0692.

Encontrou-se ainda uma falha no X Display Manager (XDM). Ele abria um socket TCP *chooserFd* mesmo se o parâmetro *DisplayManager.requestPort* estivesse definido como 0. Isso permitia que os usuários autorizados acessassem uma máquina remotamente via X, mesmo se o administrador houvesse configurado o XDM para recusar essas conexões. Embora o XFree86 4.3.0 não fosse vulnerável a esse problema, o Red Had Enterprise Linux 3 continha um patch backported que introduzia essa falha. O projeto Common Vulnerabilities and Exposures (cve.mitre.org) deu a esse problema o nome CAN-2004-0419 ■

Referência no Debian: DSA-561-1
Referência no Gentoo: GLSA 200409-34 / X
Referência no Mandrake: MDKSA-2004:099
Referência no Red Hat: RHSA-2004:478-13
Referência no Suse: SUSE-SA:2004:034

Mozilla

O Mozilla é um navegador web, cliente avançado de email e newsgroups, cliente de chat IRC e editor HTML de código aberto.

Jesse Ruderman descobriu um bug de domínio cruzado por scripts (cross-domain scripting) no Mozilla. Se um usuário for convencido a arrastar um link em JavaScript para outra página ou frame, torna-se possível a um invasor roubar ou modificar informações sigilosas desse site. Além disso, se um usuário for convencido a arrastar dois links em seqüência a outra janela (não outro frame) é possível executar código arbitrário na máquina do usuário. O projeto Common Vulnerabilities and Exposures (cve.mitre.org) deu a esse problema o nome CAN-2004-0905.

Gael Delalleau descobriu um estouro de buffer de inteiros que afeta o código de manipulação de imagens BMP no Mozilla. Um atacante poderia criar um BMP cuidadosamente preparado para derrubar o Mozilla ou executar código arbitrário quando a imagem fosse carregada. O projeto Common Vulnerabilities and Exposures (cve.mitre.org) deu a esse problema o nome CAN-2004-0904.

Georgi Guninski descobriu um estouro de pilha nas rotinas de exibição de vCards. Um invasor poderia criar um vCard malicioso cuidadosamente preparado para derrubar o Mozilla ou executar código arbitrário quando o vCard fosse carregado. O projeto Common Vulnerabilities and Exposures (cve.mitre.org) deu a esse problema o nome CAN-2004-0903.

Wladimir Palant descobriu uma falha na maneira como o JavaScript interage com a área de transferência. É possível a um invasor usar código JavaScript malicioso em uma página e roubar dados presentes na área de transferência – possivelmente, dados importantes e sigilosos. O projeto Common Vulnerabilities and Exposures (cve.mitre.org) deu a esse problema o nome CAN-2004-0908.

Georgi Guninski descobriu um estouro de buffer na área de dados do segmento (heap) na função "Send Page". Um atacante poderia construir um link de tal maneira que um usuário tentando encaminhá-lo derrubaria o Mozilla ou o faria executar código arbitrário. O projeto Common Vulnerabilities and Exposures (cve.mitre.org) deu a esse problema o nome CAN-2004-0902.

Usuários do Mozilla devem atualizar seu navegador. ■

Referência no Red Hat: RHSA-2004:486-18
Referência no Slackware: SSA:2004-266-03
Referência no SuSE: SUSE-SA:2004:036

Samba

O Samba é um servidor de arquivos e impressão para clientes SMB/CIFS.

Os desenvolvedores do Samba descobriram uma falha de negação de serviço no daemon *smbd*. Um defeito na rotina de interpretação do ASN.1 permite que um atacante envie um pacote especialmente construído durante o processo de autenticação, o que jogaria o novo processo smbd em um loop infinito. Com um certo número de pacotes é possível exaurir toda a memória disponível no servidor, resultando em negação de serviço. O projeto Common Vulnerabilities and Exposures (*cve.mitre.org*) deu a esse problema o código CAN-2004-0807.

Também foi descoberta uma falha parecida no daemon *nmbd*. É possível enviar pacotes UDP especialmente fabricados para derrubar, anonimamente, o daemon. O problema afeta apenas

os daemons *nmbd* configurados para processar logons no domínio (PDC). O projeto Common Vulnerabilities and Exposures (cve.mitre.org) deu a esse problema o nome CAN-2004-0808. ■

Referência no Debian: DSA-600-1
Referência no Mandrake: MDKSA-2004:104; MDKSA-2004:092
Referência no Red Hat: RHSA-2004:467-08
Referência no Slackware: SSA:2004-257-01
Referência no SuSE: SUSE-SA:2004:035

OpenOffice.org

OpenOffice.org é uma suíte de aplicativos para escritório que inclui processador de texto, planilha eletrônica, gerenciador de apresentação, editor de fórmula e programas de desenho.

O Secunia Research reportou uma falha na manipulação de arquivos temporários. Um usuário local mal-intencionado poderia usar essa falha para acessar o conteúdo dos documentos de outros usuários. O projeto Common Vulnerabilities and Exposures (cve.mitre.org) deu a esse problema o nome CAN-2004-0752.

Todos os usuários do OpenOffice.org são exortados a atualizar o software. ■

Referência no Mandrake: MDKSA-2004:103
Referência no Red Hat: RHSA-2004:446-08

gtk+

O pacote gtk2 contém o GIMP ToolKit (GTK+), uma biblioteca para criação de interfaces gráficas (ou GUIs) para o X Window System.

Durante os testes em uma falha previamente corrigida no Qt (CAN-2004-0691), outra foi descoberta no processador de imagens BMP do gtk2. Um invasor poderia criar uma imagem de tal forma que um aplicativo GTK+ entre em loop infinito e não responda ao usuário quando a imagem for carregada. O projeto Common Vulnerabilities and Exposures (cve.mitre.org) deu a esse problema o nome CAN-2004-0753.

Durante uma auditoria de segurança, Chris Evans descobriu estouros de buffer na pilha (stack) e na área de dados do segmento (heap) no decodificador de imagens no formato XPM. Um atacante poderia criar uma imagem XPM que derrubaria um aplicativo Gtk2 ou mesmo permitiria a execução de código arbitrário (CAN-2004-0782, CAN-2004-0783).

Chris Evans também descobriu um estouro de inteiros no decodificador de imagens ICO. Uma imagem de ícone (.ICO) poderia ser especialmente manipulada para travar o aplicativo Gtk2 ao ser aberto.(CAN-2004-0788) ■

Referência no Debian: DSA-549-1
Referência no Red Hat: RHSA-2004:466-12
Referência no Slackware: SSA:2004-266-02
Referência no SuSE: SUSE-SA:2004:033

Apache

O Apache é um servidor web (HTTP) poderoso, com muitos recursos, eficiente, livre e gratuito. Quatro falhas foram encontradas afetando versões do Apache inferiores a (e incluindo) 2.0.50.

Um teste usando a ferramenta Codenomicon HTTP foi realizada pela força-tarefa de segurança do Apache Software Foundation e pela Red Hat e descobriu uma falha de validação de entrada nas rotinas de interpretação de URIs do protocolo Ipv6. Essas falhas encontravam-se nas rotinas da biblioteca *apr-util*. Se um atacante remoto enviasse uma requisição incluindo uma URI especialmente escrita, o processo-filho httpd correspondente poderia ser forçado a travar. Essa falha não é considerada grave a ponto de permitir a execução de código arbitrário no Red Hat Enterprise Linux. Também não há perigo de ataques de negação de serviço, uma vez que outras requisições HTTP serão atendidas por outros processos-filho. O projeto Common Vulnerabilities and Exposures (cve.mitre.org) deu a esse problema o nome CAN-2004-0786.

O Centro de Incidentes de IT da Suécia (Swedish IT Incident Centre – SITIC) divulgou um estouro de buffer na expansão de variáveis de ambiente durante a interpretação de arquivos de configuração. Essa falha permitiria a um usuário ganhar privilégios do usuário apache se um processo *httpd* pudesse ser forçado a interpretar um arquivo *.htaccess* cuidadosamente preparado. O projeto Common Vulnerabilities and Exposures deu a esse problema o código CAN-2004-0747.

Outra falha foi descoberta no módulo *mod_ssl*. Pode ser explorada se o servidor for configurado como intermediário (proxy) de um servidor SSL remoto. Um servidor remoto malicioso de SSL pode forçar um processo-filho *httpd* a travar pelo envio de uma resposta com um cabeçalho adulterado. Estima-se que não seja possível executar código arbitrário por essa falha. Também não há perigo de ataques de negação de serviço, uma vez que outras requisições HTTP serão atendidas por outros processos-filho. O projeto Common Vulnerabilities and Exposures (cve.mitre.org) deu a esse problema o nome CAN-2004-0751.

Outra falha, descoberta no módulo *mod_dav*, pode ser explorada se o acesso por WebDAV estiver configurado. Um cliente remoto, autorizado a usar o método LOCK, pode forçar um processo-filho *httpd* a travar pelo envio de uma seqüência peculiar de requisições LOCK. Não é possível executar código arbitrário com essa falha. Também não há perigo de ataques de negação de serviço, uma vez que outras requisições HTTP serão atendidas por outros processos-filho. O projeto Common Vulnerabilities and Exposures deu a esse problema o código CAN-2004-0809. ■

Referência no Mandrake: MDKSA-2004:096
Referência no Red Hat: RHSA-2004:463-09
Referência no SuSE: SUSE-SA:2004:032

SpamAssassin

O SpamAssassin é um filtro local contra spam e mensagens não solicitadas. Uma falha de negação de serviço foi encontrada no SpamAssassin em versões inferiores à 2.64. Um atacante poderia escrever uma mensagem de email elaborada de forma a provocar o congelamento do SpamAssassin, potencialmente evitando a filtragem ou mesmo a entrega de email. O projeto Common Vulnerabilities and Exposures deu a esse problema o nome CAN-2004-0796. Usuários do SpamAssassin devem atualizar seu software. ■

Referência no Red Hat: RHSA-2004:451-05

Webmin

O webmin é uma ferramenta básica de administração. Ludwig Nussel descobriu um problema quando um diretório temporário é usado mas seu dono não é verificado. Isso pode ser usado para criar um diretório arbitrário e colocar nele links simbólicos perigosos. ■

Referência no Debian: DSA-544-1
Referência no Mandrake: MDKSA-2004:101