

Raport o najnowszych zagrożeniach

■ jitterbug

Steve Kemp wykrył problem związany z bezpieczeństwem w pakiecie jitterbug – prostym, opartym na CGI narzędziu do śledzenia błędów i raportowania. Niestety program nie sprawdza poprawności danych wejściowych, co umożliwia atakującemu wykonanie poleceń na serwerze, który utrzymuje bazę błędów. Wagę błędu zmniejsza fakt, że atak może być wykonany jedynie z konta użytkownika innego niż gość, a konto tego użytkownika musi być oznaczone przez administratora jako zaufane (opcja „trusted”).

Opis błędu dla Debiana: DSA-420-1 jitterbug – improperly sanitized input

■ CVS

CVS jest systemem kontroli wersji często spotykanym do zarządzania repozytorium kodu źródłowego projektów programistycznych. W wersjach CVS, starszych niż 1.11.10, nieprawidłowe wywołanie modułu może spowodować, że serwer CVS będzie usiłował utworzyć pliki lub katalogi w głównym katalogu systemu plików. Tym niemniej, standardowy mechanizm uprawnień dostępu do plików powinien uchronić przed utworzeniem tych katalogów i plików. Projekt Common Vulnerabilities and Exposures przypisał temu błędowi kod CAN-2003-0977.

Opis błędu dla Red Hat: RHSA-2004:003-04

■ Jądro 2.4.23 i poprzednie

Funkcja `do_mremap()` jest używana przez jądro Linuksa do zarządzania (przeniesienia, zmiany rozmiaru) tzw. obszarów pamięci wirtualnej – Virtual Memory Areas (VMAs). Paul Starzetz wykrył, że wykorzystując nieprawidłową funkcję kontrolną `do_mremap()` podczas zmiany mapowania pamięci, możliwe jest utworzenie VMA o wielkości 0. W normalnej sytuacji funkcja `do_mremap()` pozostawia pustą przestrzeń pamięci dla jednej strony i tworzy dodatkowe dwie strony VMA. W przypadku sytuacji opisanej przez exploit, jest co prawda tworzona strona w pamięci, ale ma ona zerową długość. Powoduje to załamanie systemu zarządzania pamięcią w jądrze Linuksa, co umożliwia lokalnym użytkownikom przejęcie uprawnień użytkownika root.

Opis błędu dla SuSE: SuSE-SA:2004:001

Opis błędu dla Mandrake:

MDKSA-2004:001: kernel

Opis błędu dla Red Hat: RHSA-2003:417-08

■ FSP

Wykryto błąd w programie fsp, jest to program narzędziowy dla usługi File Service Protocol (FSP), błąd umożliwia wyjście użytkownika poza główny katalog FSP (CAN-2003-1022), może również spowodować przepełnienie bufora, co może umożliwić wykonanie dowolnego kodu binarnego (CAN-2004-0011).

Opis błędu dla Debiana: DSA-416-1 fsp

– buffer overflow, directory traversal

■ irssi

W wersji programu irssi, wcześniejszych niż 0.8.9, wykryto błąd umożliwiający zdalnemu użytkownikowi zawieszenie sesji irssi innego użytkownika, o ile klient ten nie jest uruchomiony na platformie innej niż x86 lub gdy któryś z pluginów albo skryptów wysłał sygnał „gui print text”.

Opis błędu dla Mandrake:

MDKSA-2003:117: irssi

Źródła informacji o bezpieczeństwie dla najważniejszych dystrybucji Linuksa

Dystrybucja	Źródła informacji	Komentarz
Debian	Info: http://www.debian.org/security/ Lista: http://lists.debian.org/debian-security-announce/ Kod informacji: DSA-... ¹⁾	Bieżące informacje o bezpieczeństwie znajdują się na stronie domowej projektu. Informacje o problemach są rozsyłane w postaci listów w formacie HTML z adresami URL, pod którymi można znaleźć łatkę oraz do odpowiednich wątków listy dyskusyjnej.
Gentoo	Forum: http://forums.gentoo.org Lista: http://www.gentoo.org/main/en/lists.xml Kod informacji: GLSA-... ¹⁾	Niestety projekt Gentoo nie posiada strony WWW z aktualizacjami i informacjami o bezpieczeństwie. Gentoo Forum jest zatem jedynym źródłem informacji.
Mandrake	Info: http://www.mandrakesecure.net Lista: http://www.mandrakesecure.net/en/mlist.php Kod informacji: MDKSA-... ¹⁾	Firma MandrakeSoft prowadzi własną stronę poświęconą bezpieczeństwu, zawiera ona między innymi bieżące informacje o bezpieczeństwie i odsyła do interesujących wątków list dyskusyjnych.
Red Hat	Info: http://www.redhat.com/errata/ Lista: http://www.redhat.com/mailling-lists/ Kod informacji: RHSA-... ¹⁾	Informacje o bezpieczeństwie nazywane są Errata i są pogrupowane stosownie do wersji, której dotyczą. Informacje o problemach są przesyłane w postaci listów w formacie HTML z adresami URL do łatek.
Slackware	Info: http://www.slackware.com/security/ Lista: http://www.slackware.com/lists/(slackware-security) Kod informacji: [slackware-security]... ¹⁾	Strona startowa zawiera adresy do archiwum listy dyskusyjnej. Jest to jedyne źródło informacji o bezpieczeństwie Slackware podawane przez producenta.
Suse	Info: http://www.suse.de/uk/private/support/security/ Łatki: http://www.suse.de/uk/private/download/updates/ Lista: suse-security-announce Kod informacji: SUSE-SA-... ¹⁾	Na stronie głównej można znaleźć najnowsze informacje dotyczące bezpieczeństwa oraz adresy list dyskusyjnych. Do łatek bezpieczeństwa dołączony jest zawsze krótki opis problemu, który łatka rozwiązuje.

¹⁾ Żeby otrzymywać list z alertami bezpieczeństwa, wyślij list ze słowem „security” w tytule maila.

■ Lftp

Ulf Harnhammar wykrył dwa błędy w programie lftp, umożliwiające zdalne przepełnienie bufora. Lftp jest elastycznym i posiadającym duże możliwości klientem FTP.

Jeśli w czasie połączenia lftp z serwerami HTTP lub HTTPS zostanie wykonane polecenie takie jak „ls” lub „rels”, specjalnie spreparowany katalog na serwerze może spowodować przepełnienie bufora w funkcji obsługującej protokół HTTP. Może to doprowadzić do uruchomienia dowolnego kodu po stronie klienta. Ten exploit nie ma wpływu na bezpieczeństwo serwera, a napastnik może uzyskać dostęp jedynie do konta użytkownika korzystającego z lftp. Błąd występuje w lftp w wersjach od 2.3.0 do 2.6.9 i został poprawiony od wersji 2.6.10. ■

Opis błędu dla SuSE: SuSE-SA:2003:051

Opis błędu dla Mandrake:

MDKSA-2003:116: lftp

Opis błędu dla Red Hat: RHSA-2003:403-07

Opis błędu dla Debiana: DSA-406-1 lftp

– buffer overflow

■ phpgroupware

Autorzy phpgroupware, opartego na WWW systemu pracy grupowej napisanego w PHP, odkryli w swoim oprogramowaniu kilka błędów. Projekt Common Vulnerabilities and Exposures zidentyfikował następujące zagrożenia:

CAN-2004-0016 – W module „calendar” funkcja „save extension” nie została zdefiniowana dla plików z opisem dni wolnych. W rezultacie, skrypty PHP po stronie serwera mogą być umieszczane w katalogach, tak że można zdalnie nakazać ich wykonanie przez serwer WWW. Na szczęście można to łatwo rozwiązać, nadając rozszerzenie „.txt” plikom z definicjami dni wolnych.

CAN-2004-0017 – problemy z zagrożeniami typu „SQL injection” (non-escaping of values used in SQL strings) w modułach „calendar” i „infolog”. Dodatkowo, osoba opiekująca się pakietami w wersjach dla Debiana poprawiła prawa dostępu („world writable”) do katalogów aplikacji, które zostały przypadkowo przyznane przez starszą wersję skryptu postinst z pakietu dpkg. ■

Opis błędu dla Debiana:

DSA-419-1 phpgroupware

– missing filename sanitizing, SQL injection

■ tcpdump

Znaleziono kilka poważnych dziur bezpieczeństwa w tcpdump, narzędziu służąc-

ym badaniu ruchu w sieci. Jeśli podatna wersja tcpdump spróbuje sprawdzić odpowiednio spreparowany pakiet, możliwe jest wykorzystanie kilku błędów przepełnienia bufora do zawieszenia tcpdump lub potencjalne uruchomienie własnego kodu z prawami procesu tcpdump.

W stabilnej dystrybucji (woody) powyższe problemy zostały wyeliminowane w wersji 3.6.2-2.7. W dystrybucji niestabilnej (sid) powyższe problemy będą usunięte niedługo. Zalecana jest aktualizacja pakietu tcpdump. ■

DSA-425-1 tcpdump – kilka naruszeń bezpieczeństwa

W słowniku CVE Mitre-a CAN-2003-1029,

CAN-2003-0989, CAN-2004-0055,

CAN-2004-0057

Baza danych błędów, porad i incydentów

CERT: VU#174086, VU#955526,

VU#738518

■ Midnight Commander

Znaleziono naruszenie bezpieczeństwa w Midnight Commander (mc), popularnym znakowym menedżerze plików, za pomocą którego złośliwe archiwum (takie jak np. plik.tar) może spowodować uruchomienie własnego kodu podczas otwierania takiego pliku w Midnight Commander.

W stabilnej dystrybucji (woody) powyższy problem został wyeliminowany w wersji 4.5.55-1.2woody2. W dystrybucji niestabilnej (sid) powyższy problem został wyeliminowany w wersji 1:4.6.0-4.6.1-pre1-1. Zalecana jest aktualizacja pakietu mc. ■

Opis błędu dla Debiana DSA-424-1

mc – przepełnienie bufora

W słowniku CVE Mitre-a CAN-2003-1023

■ netpbm-free

netpbm to zestaw narzędzi konwertujących pliki graficzne składający się z kilku pojedynczych programów. Wiele z tych programów tworzy pliki tymczasowe w niepewny sposób, umożliwiając tym samym atakującemu lokalnie nadpisanie plików z prawami użytkownika wywołującego podatną wersję netpbm.

W stabilnej dystrybucji (woody) powyższe problemy zostały wyeliminowane w wersji 2:9.20-8.4. W dystrybucji niestabilnej (sid) powyższe problemy zostały wyeliminowane w wersji 2:9.25-9. Zalecana jest aktualizacja pakietu netpbm-free. ■

Opis błędu dla Debiana DSA-426-1

netpbm-free – niepewne pliki tymczasowe

Baza danych błędów, porad

i incydentów CERT: VU#487102

W słowniku CVE Mitre-a CAN-2003-0924

■ slocate

Znaleziono naruszenie bezpieczeństwa w slocate, programie do indeksowania i wyszukiwania plików, za pomocą którego odpowiednio spreparowana baza danych może przepełnić bufor oparty na stosie. Ta podatność może być wykorzystana przez atakującego lokalnie do uzyskania praw grupy „slocate”, która ma dostęp do globalnej bazy danych zawierającej listę ścieżek wszystkich plików w systemie włącznie z tymi, które powinny być widoczne tylko dla uprzywilejowanych użytkowników.

Problem ten, a także podobne potencjalne problemy, został rozwiązany poprzez modyfikację slocate tak aby program tracił przywileje zanim zacznie czytać w bazie danych użytkownika. W stabilnej dystrybucji (woody) powyższy problem został wyeliminowany w wersji 2.6-1.3.2.

W dystrybucji niestabilnej (sid) powyższy problem będzie poprawiony niedługo. Informacja o stanie tego problemu przypisana jest do błędu Debiana #226103. Zalecamy aktualizację pakietu slocate. ■

Opis błędu dla Debiana – DSA-428-1

slocate – przepełnienie bufora

Odnośniki do baz danych na temat

bezpieczeństwa:

W słowniku CVE Mitre-a CAN-2003-0848.

■ mod-auth-shadow

David B. Harris znalazł problem w mod-auth-shadow, modułu Apache dokonującego autentyfikacji użytkowników w bazie danych haseł typu shadow, gdzie stan przedawnienia konta użytkownika i jego hasła nie zostaje egzekwowany. Ta podatność pozwala takiemu użytkownikowi na prawidłową autentyfikację, podczas gdy próba taka powinna być odrzucona z powodu przedawnionych parametrów. W stabilnej dystrybucji (woody) powyższy problem został wyeliminowany w wersji 1.3-3.1woody.1. W dystrybucji niestabilnej (sid) powyższy problem został wyeliminowany w wersji 1.4-1. Zalecana jest aktualizacja pakietu mod-auth-shadow. ■

Opis błędu dla Debiana – DSA-421-1

mod-auth-shadow – przedawnienie hasła

Odnośniki do baz danych na temat

bezpieczeństwa:

W słowniku CVE Mitre-a CAN-2004-0041.