Portaudit - мониторинг уязвимостей в системе

Опубликовано muff в Ср, 2012-01-04 05:11

Думаю всем известно, что ПО во **FreeBSD** поставляется с базовой системой, а также устанавливается из системы портов. Если уследить за "дырками в секьюрности" самой системы еще представляется возможным, то следить за всеми найденными уязвимостями в ПО, установленном из системы портов - просто нереально.

На помощь приходит утилита **portaudit**, которая проверяет установленное програмное обеспечение на наличие уязвимостей. **Portaudit** будет каждый день проверять наличие уязвимостей в установленном ПО и присылать отчет на почту. По умолчанию **portaudit** интегрируется с **periodic**, чтобы запускаться ежедневно. Во время работы она загружается последняя версия базы данных уязвимостей с сайта **http://www.freebsd.org** и сравнивает со списком установленных портов. Результаты проверки отправляются по электронной почте пользователю **root** с отчетом **periodic** и URL-адресами, по которым можно найти описание выявленных проблем и пути их устранения.

Выполним установку **portaudit** из системы портов:

```
# cd /usr/ports/ports-mgmt/portaudit/ && make install clean && rehash
```

Установка выполнилась очень быстро. В конце установки порт "вывел" подсказку:

```
===>  To check your installed ports for known vulnerabilities now, do:

    /usr/local/sbin/portaudit -Fda
```

Итак, проверим на тестовом сервере, какие уязвимости будут обнаружены:

```
# /usr/local/sbin/portaudit -Fda
  auditfile.tbz                                 100% of   71 kB   32 kBps
New database installed.
Database created: среда,  4 января 2012 г. 03:45:00 (EET)
Affected package: proftpd-1.3.3c_1
Type of problem: proftpd -- arbitrary code execution vulnerability with chroot.
Reference: http://portaudit.FreeBSD.org/022a4c77-2da4-11e1-b356-00215c6a37bb.html

Affected package: phpMyAdmin-3.1.3
Type of problem: phpmyadmin -- Local file inclusion.
Reference: http://portaudit.FreeBSD.org/1f6ee708-0d22-11e1-b5bd-14dae938ec40.html

Affected package: libxml2-2.7.3
Type of problem: libxml -- Integer overflow.
Reference: http://portaudit.FreeBSD.org/ce4b3af8-0b7c-11e1-846b-00235409fd3e.html

Affected package: freetype2-2.3.7
Type of problem: freetype -- Some type 1 fonts handling vulnerabilities.
Reference: http://portaudit.FreeBSD.org/54075e39-04ac-11e1-a94e-bcaec565249c.html

Affected package: quagga-0.99.12
Type of problem: quagga -- multiple vulnerabilities.
Reference: http://portaudit.FreeBSD.org/ab9be2c8-ef91-11e0-ad5a-00215c6a37bb.html

Affected package: phpMyAdmin-3.1.3
Type of problem: phpmyadmin -- multiple XSS vulnerabilities.
Reference: http://portaudit.FreeBSD.org/e44fe906-df27-11e0-a333-001cc0a36e12.html
```

Affected package: ca_root_nss-3.11.9_2
Type of problem: ca_root_nss -- extraction of explicitly-untrusted certificates into trust bundle.
Reference: http://portaudit.FreeBSD.org/1b27af46-d6f6-11e0-89a6-080027ef73ec.html

Affected package: ca_root_nss-3.11.9_2
Type of problem: nss/ca_root_nss -- fraudulent certificates issued by DigiNotar.nl.
Reference: http://portaudit.FreeBSD.org/aa5bc971-d635-11e0-b3cf-080027ef73ec.html

Affected package: apache-2.2.11_3
Type of problem: apache -- Range header DoS vulnerability.
Reference: http://portaudit.FreeBSD.org/7f6108d2-cea8-11e0-9d58-0800279895ea.html

Affected package: phpMyAdmin-3.1.3
Type of problem: phpmyadmin -- multiple XSS vulnerabilities.
Reference: http://portaudit.FreeBSD.org/75e26236-ce9e-11e0-b26a-00215c6a37bb.html

Affected package: freetype2-2.3.7
Type of problem: freetype2 -- execute arbitrary code or cause denial of service.
Reference: http://portaudit.FreeBSD.org/5d374b01-c3ee-11e0-8aa5-485d60cb5385.html

Affected package: phpMyAdmin-3.1.3
Type of problem: phpmyadmin -- multiple vulnerabilities.
Reference: http://portaudit.FreeBSD.org/d79fc873-b5f9-11e0-89b4-001ec9578670.html

Affected package: phpMyAdmin-3.1.3
Type of problem: phpmyadmin -- multiple vulnerabilities.
Reference: http://portaudit.FreeBSD.org/7e4e5c53-a56c-11e0-b180-00216aa06fc2.html

Affected package: quagga-0.99.12
Type of problem: quagga -- two DoS vulnerabilities.
Reference: http://portaudit.FreeBSD.org/b2a40507-5c88-11e0-9e85-00215af774f0.html

Affected package: phpMyAdmin-3.1.3
Type of problem: phpMyAdmin -- multiple vulnerabilities.
Reference: http://portaudit.FreeBSD.org/cd68ff50-362b-11e0-ad36-00215c6a37bb.html

Affected package: php52-5.2.14_1
Type of problem: php -- multiple vulnerabilities.
Reference: http://portaudit.FreeBSD.org/2b6ed5c7-1a7f-11e0-b61d-000c29d1636d.html

Affected package: php52-zip-5.2.14_1
Type of problem: php-zip -- multiple Denial of Service vulnerabilities.
Reference: http://portaudit.FreeBSD.org/2a41233d-10e7-11e0-becc-0022156e8794.html

Affected package: php52-filter-5.2.14_1
Type of problem: php-filter -- Denial of Service.
Reference: http://portaudit.FreeBSD.org/c623f058-10e7-11e0-becc-0022156e8794.html

Affected package: php52-5.2.14_1
Type of problem: php -- NULL byte poisoning.
Reference: http://portaudit.FreeBSD.org/3761df02-0f9c-11e0-becc-0022156e8794.html

Affected package: php52-5.2.14_1
Type of problem: php -- open_basedir bypass.
Reference: http://portaudit.FreeBSD.org/73634294-0fa7-11e0-becc-0022156e8794.html

Affected package: php52-5.2.14_1
Type of problem: php -- corruption of $GLOBALS and $this variables via extract() method.
Reference: http://portaudit.FreeBSD.org/f3148a05-0fa7-11e0-becc-0022156e8794.html

Affected package: phpMyAdmin-3.1.3
Type of problem: phpMyAdmin -- XSS attack in database search.
Reference: http://portaudit.FreeBSD.org/753f8185-5ba9-42a4-be02-3f55ee580093.html

Affected package: wget-1.11.4
Type of problem: wget -- multiple HTTP client download filename vulnerability.
Reference: http://portaudit.FreeBSD.org/d754b7d2-b6a7-11df-826c-e464a695cb21.html

Affected package: quagga-0.99.12
Type of problem: quagga -- stack overflow and DoS vulnerabilities.
Reference: http://portaudit.FreeBSD.org/167953a4-b01c-11df-9a98-0015587e2cc1.html

Affected package: phpMyAdmin-3.1.3
Type of problem: phpmyadmin -- Several XSS vulnerabilities.
Reference: http://portaudit.FreeBSD.org/274922b8-ad20-11df-af1f-00e0814cab4e.html

Affected package: apache-2.2.11_3
Type of problem: apache -- Remote DoS bug in mod_cache and mod_dav.
Reference: http://portaudit.FreeBSD.org/28a7310f-9855-11df-8d36-001aa0166822.html

Affected package: sudo-1.6.9.20
Type of problem: sudo -- Secure path vulnerability.
Reference: http://portaudit.FreeBSD.org/d42e5b66-6ea0-11df-9c8d-00e0815b8da8.html

Affected package: joomla15-1.5.8
Type of problem: joomla -- multiple vulnerabilities.
Reference: http://portaudit.FreeBSD.org/8d10038e-515c-11df-83fb-0015587e2cc1.html

Affected package: curl-7.19.4
Type of problem: curl -- libcurl buffer overflow vulnerability.
Reference: http://portaudit.FreeBSD.org/c8c31c41-49ed-11df-83fb-0015587e2cc1.html

Affected package: sudo-1.6.9.20
Type of problem: sudo -- Privilege escalation with sudoedit.
Reference: http://portaudit.FreeBSD.org/1a9f678d-48ca-11df-85f8-000c29a67389.html

Affected package: sudo-1.6.9.20
Type of problem: sudo -- Privilege escalation with sudoedit.
Reference: http://portaudit.FreeBSD.org/018a84d0-2548-11df-b4a3-00e0815b8da8.html

Affected package: libvorbis-1.2.0_3,3
Type of problem: libvorbis -- multiple vulnerabilities.
Reference: http://portaudit.FreeBSD.org/94edff42-d93d-11de-a434-0211d880e350.html

Affected package: gd-2.0.35,1
Type of problem: gd -- '_gdGetColors' remote buffer overflow vulnerability.
Reference: http://portaudit.FreeBSD.org/4e8344a3-ca52-11de-8ee8-00215c6a37bb.html

Affected package: phpMyAdmin-3.1.3
Type of problem: phpmyadmin -- XSS and SQL injection vulnerabilities.
Reference: http://portaudit.FreeBSD.org/4769914e-b844-11de-b159-0030843d3802.html

Affected package: apache-2.2.11_3
Type of problem: apache22 -- several vulnerability.
Reference: http://portaudit.FreeBSD.org/e15f2356-9139-11de-8f42-001aa0166822.html

Affected package: joomla15-1.5.8
Type of problem: joomla15 -- com_mailto Timeout Issue.

```
Reference: http://portaudit.FreeBSD.org/739b94a4-838b-11de-938e-003048590f9e.html

Affected package: phpMyAdmin-3.1.3
Type of problem: phpmyadmin -- XSS vulnerability.
Reference: http://portaudit.FreeBSD.org/ba73f494-65a8-11de-aef5-001c2514716c.html

Affected package: joomla15-1.5.8
Type of problem: joomla -- multiple vulnerabilities.
Reference: http://portaudit.FreeBSD.org/bdccd14b-5aac-11de-a438-003048590f9e.html

Affected package: apache-2.2.11_3
Type of problem: apr -- multiple vulnerabilities.
Reference: http://portaudit.FreeBSD.org/eb9212f7-526b-11de-bbf2-001b77d09812.html

Affected package: freetype2-2.3.7
Type of problem: freetype2 -- multiple vulnerabilities.
Reference: http://portaudit.FreeBSD.org/20b4f284-2bfc-11de-bdeb-0030843d3802.html

Affected package: phpMyAdmin-3.1.3
Type of problem: phpmyadmin -- insufficient output sanitizing when generating configuration file.
Reference: http://portaudit.FreeBSD.org/1a0e4cc6-29bf-11de-bdeb-0030843d3802.html

Affected package: phpMyAdmin-3.1.3
Type of problem: phpmyadmin -- insufficient output sanitizing when generating configuration file.
Reference: http://portaudit.FreeBSD.org/06f9174f-190f-11de-b2f0-001c2514716c.html

42 problem(s) in your installed packages found.

You are advised to update or deinstall the affected package(s) immediately.
```

М-дя... Обнаружено 42 уязвимости. Кажется пора и на тестовом сервере следить за актуальностью установленного ПО.

Некоторые из доступных опций запуска:

- **portaudit -a** - вывод отчета о уязвимостях в установленных портах.
- **portaudit -C** - вывод отчета о уязвимостях порта, находящегося в текущей директории.
- **portaudit -F** - загрузить последнюю базу
- **portaudit -q** - "тихий" режим
- **portaudit -d** - проверка, когда последний раз выполнялась загрузка базы
- **portaudit -V** - вывод версии
- **portaudit -v** - режим отладки
- **portaudit -X days** - загружает базу, если она старше "days"
- **portaudit -f <file>** - проверка пакетов, перечисленных в файле
- **portaudit <пакет>** - информация о уязвимостях конкретного пакета

Также стоит иметь ввиду, что система запускает **portaudit** при каждой попытке установки ПО из системы портов. Если для порта обнаружены проблемы с безопасностью, то установка будет остановлена. Если же установка небезопасного порта все же необходима, то для обхода запрета в **/etc/make.conf** добавляем такую опцию сборки:

```
DISABLE_VULNERABILITIES=yes
```

А для того, чтобы легко обновлять установленные порты, советую "подружиться" с такой утилитой, как portupgrade **[1]**.

Источник (получено *2025-03-30 09:24*):
http://muff.kiev.ua/content/portaudit-monitoring-uyazvimostei-v-sisteme

Ссылки:
[1] http://muff.kiev.ua/content/portupgrade-korrektnoe-obnovlenie-ustanovlenogo-softa