pkgsrc-security

Vulnerability management or the frustrations for lack of

Sevan Janiyan
sevan@NetBSD.org
@sevanjaniyan

Team of 4

weekly rota - per person shifts

Sometimes it rains

&

Sometimes there’s drought

(only for a shift)

Mandrake / Mandriva
Mageia

pkg-vulnerabilities file lives
On ftp.NetBSD.org
In /pub/NetBSD/packages/vulns

```
# package                     type of exploit        URL
mDNSResponder<625.41.2    denial-of-service    http://www……
```

Tediousness

OpenSSL

PHP

Java

Qemu/Xen/Kvm

Flash

Flash, flash, flash
die, die, die

Disclosure / Advisory process is clumsy

Non security conscious projects
Amplified noise
Advanced Information Security Corp
http://www.securityfocus.com/archive/1/535303

Git
CVE-2016-2324
CVE-2016-2315

http://seclists.org/oss-sec/2016/q1/645

Oh………………………… Big mistake. I might advertised too soon.

I saw changes were pushed in master, so I thought the next version (which was 2.7.1) would be the one which will include the fix.

But as pointed out on https://security-tracker.debian.org/tracker/CVE-2016-2324 no versions including the fixes were released yet, and even 2.7.3 still include path_name(). I didn't checked the code (Sorrrry).

Jasper

CVE-2008-3520

CVE-2008-3522

CVE-2011-4516

CVE-2011-4517

CVE-2014-8137

CVE-2014-9029

“tidy up a few warnings. with help from naddy@“ - espie@

OCaml
CVE-2015-8869

OCamel before 4.03.0 does not properly handle sign extensions, which allows remote attackers to conduct buffer overflow attacks or obtain sensitive information as demonstrated by a long string to the String.copy function.

Where are the official OCaml advisories published at?