FreeNAS - Bug #24885

Update system packages

06/28/2017 08:25 AM - Mike Kelly

Status:	Resolved		
Priority:	Expected		
Assignee:	Alexander Motin		
Category:	OS		
Target version:	11.1-BETA1		
Seen in:	11.0	**Needs Merging:**	Yes
Severity:	New	**Needs Automation:**	No
Reason for Closing:		**Support Suite Ticket:**	n/a
Reason for Blocked:		**Hardware Configuration:**	
Needs QA:	No	**ChangeLog Required:**	No
Needs Doc:	Yes		

Description

pkg audit -F shows a lot of packages that are part of the base FreeNAS install with vulnerabilities.

It seems that, due to some part of the design or configuration of FreeNAS, a usual pkg upgrade does not function.

Listed vulnerabilities:

```
apache24-2.4.25_1 is vulnerable:

Apache httpd -- several vulnerabilities

CVE: CVE-2017-7679
CVE: CVE-2017-7668
CVE: CVE-2017-7659
CVE: CVE-2017-3169

CVE: CVE-2017-3167

WWW: https://vuxml.FreeBSD.org/freebsd/0c2db2aa-5584-11e7-9a7d-b499baebfeaf.html

curl-7.52.1 is vulnerable:

cURL -- TLS session resumption client cert bypass (again)
CVE: CVE-2017-7468

WWW: https://vuxml.FreeBSD.org/freebsd/3e2e9b44-25ce-11e7-a175-939b30e0836d.html

curl-7.52.1 is vulnerable:
cURL -- potential memory disclosure
CVE: CVE-2017-7407
WWW: https://vuxml.FreeBSD.org/freebsd/04f29189-1a05-11e7-bc6e-b499baebfeaf.html

curl-7.52.1 is vulnerable:
cURL -- ocsp status validation error
CVE: CVE-2017-2629
WWW: https://vuxml.FreeBSD.org/freebsd/311e4b1c-f8ee-11e6-9940-b499baebfeaf.html

openvpn-2.3.12_1 is vulnerable:
OpenVPN -- two remote denial-of-service vulnerabilities
CVE: CVE-2017-7479
CVE: CVE-2017-7478
```

```
WWW: https://vuxml.FreeBSD.org/freebsd/04cc7bd2-3686-11e7-aa64-080027ef73ec.html

openvpn-2.3.12_1 is vulnerable:
OpenVPN -- several vulnerabilities
CVE: CVE-2017-7522
CVE: CVE-2017-7521
CVE: CVE-2017-7520
CVE: CVE-2017-7512
CVE: CVE-2017-7508
WWW: https://vuxml.FreeBSD.org/freebsd/9f65d382-56a4-11e7-83e3-080027ef73ec.html

icu-57.1,1 is vulnerable:
icu -- multiple vulnerabilities
CVE: CVE-2017-7868
CVE: CVE-2017-7867
WWW: https://vuxml.FreeBSD.org/freebsd/607f8b57-7454-42c6-a88a-8706f327076d.html

graphite2-1.3.8 is vulnerable:
graphite2 -- out-of-bounds write with malicious font
CVE: CVE-2017-5436
WWW: https://vuxml.FreeBSD.org/freebsd/cf133acc-82e7-4755-a66a-5ddf90dacbe6.html

freetype2-2.6.3 is vulnerable:
freetype2 -- buffer overflows
CVE: CVE-2017-8287
CVE: CVE-2017-8105
WWW: https://vuxml.FreeBSD.org/freebsd/4a088d67-3af2-11e7-9d75-c86000169601.html

nss-3.28 is vulnerable:
NSS -- multiple vulnerabilities
CVE: CVE-2017-5462
CVE: CVE-2017-5461
WWW: https://vuxml.FreeBSD.org/freebsd/4cb165f0-6e48-423e-8147-92255d35c0f7.html

openssl-1.0.2j_1,1 is vulnerable:
OpenSSL -- multiple vulnerabilities
CVE: CVE-2017-3732
CVE: CVE-2017-3731
CVE: CVE-2017-3730
CVE: CVE-2016-7055
WWW: https://vuxml.FreeBSD.org/freebsd/d455708a-e3d3-11e6-9940-b499baebfeaf.html

libevent2-2.0.22_1 is vulnerable:
libevent -- multiple vulnerabilities
CVE: CVE-2016-10197
CVE: CVE-2016-10196
CVE: CVE-2016-10195
WWW: https://vuxml.FreeBSD.org/freebsd/b8ee7a81-a879-4358-9b30-7dd1bd4c14b1.html

gnutls-3.4.15 is vulnerable:
GnuTLS -- Memory corruption vulnerabilities
WWW: https://vuxml.FreeBSD.org/freebsd/0c5369fc-d671-11e6-a9a5-b499baebfeaf.html

gnutls-3.4.15 is vulnerable:
GnuTLS -- Denial of service vulnerability
WWW: https://vuxml.FreeBSD.org/freebsd/b33fb1e0-4c37-11e7-afeb-0011d823eebd.html

10 problem(s) in the installed packages found.
```

History

#1 - 06/28/2017 09:36 AM - Alexander Motin

- Status changed from Unscreened to Resolved

- Priority changed from No priority to Expected

- Target version set to 11.1

Yes, it is quite possible, since packages were not updated between 9.10.2 and 11.0 and are now 6+ months old, since amount of changes was too big already. They are already updated in nightly builds for further FreeNAS 11.1. I haven't looked on every reported CVE, but at least some of them seem not applicable to FreeNAS.

#2 - 08/09/2017 10:29 AM - Dru Lavigne

- Private changed from Yes to No

#3 - 09/01/2017 11:25 AM - Dru Lavigne

- Subject changed from Multiple Insecure Packages to Update system packages

#4 - 09/26/2017 03:51 PM - Dru Lavigne

- Target version changed from 11.1 to 11.1-BETA1

#5 - 10/30/2017 09:45 AM - Bonnie Follweiler

Alexander, given the output from pkg audit, are these vulnerabilities related tp FreeNAS or do I mark this ticket "test passes"?

I ran pkg Audit and got the following output:
vulnxml file up-to-date
apache24-2.4.27 is vulnerable:
Apache -- HTTP OPTIONS method can leak server memory
CVE: CVE-2017-9798
WWW: https://vuxml.FreeBSD.org/freebsd/76b085e2-9d33-11e7-9260-000c292ee6b8.html

python27-2.7.13_7 is vulnerable:
Python 2.7 -- multiple vulnerabilities
CVE: CVE-2017-9233
CVE: CVE-2016-9063
CVE: CVE-2016-5300
CVE: CVE-2016-4472
CVE: CVE-2016-0718
CVE: CVE-2012-0876
WWW: https://vuxml.FreeBSD.org/freebsd/9164f51e-ae20-11e7-a633-009c02a2ab30.html

curl-7.55.1 is vulnerable:
cURL -- out of bounds read
CVE: CVE-2017-1000254
WWW: https://vuxml.FreeBSD.org/freebsd/ccace707-a8d8-11e7-ac58-b499baebfeaf.html

curl-7.55.1 is vulnerable:
cURL -- out of bounds read
CVE: CVE-2017-1000257
WWW: https://vuxml.FreeBSD.org/freebsd/143ec3d6-b7cf-11e7-ac58-b499baebfeaf.html

openvpn-2.4.3 is vulnerable:
OpenVPN -- out-of-bounds write in legacy key-method 1
CVE: CVE-2017-12166
WWW: https://vuxml.FreeBSD.org/freebsd/3dd6ccf4-a3c6-11e7-a52e-0800279f2ff8.html

perl5-5.24.2 is vulnerable:
perl -- multiple vulnerabilities
CVE: CVE-2017-12883
CVE: CVE-2017-12837
CVE: CVE-2017-12814
WWW: https://vuxml.FreeBSD.org/freebsd/d9e82328-a129-11e7-987e-4f174049b30a.html

nss-3.32 is vulnerable:
nss -- Use-after-free in TLS 1.2 generating handshake hashes
CVE: CVE-2017-7805
WWW: https://vuxml.FreeBSD.org/freebsd/e71fd9d3-af47-11e7-a633-009c02a2ab30.html

dnsmasq-2.77_1,1 is vulnerable:
dnsmasq -- multiple vulnerabilities
CVE: CVE-2017-13704
CVE: CVE-2017-14496
CVE: CVE-2017-14495
CVE: CVE-2017-14494
CVE: CVE-2017-14493

CVE: CVE-2017-14492
CVE: CVE-2017-14491
WWW: https://vuxml.FreeBSD.org/freebsd/b77b5646-a778-11e7-ac58-b499baebfeaf.html

wget-1.19.1_1 is vulnerable:
wget -- Heap overflow in HTTP protocol handling
CVE: CVE-2017-13090
WWW: https://vuxml.FreeBSD.org/freebsd/d77ceb8c-bb13-11e7-8357-3065ec6f3643.html

wget-1.19.1_1 is vulnerable:
wget -- Stack overflow in HTTP protocol handling
CVE: CVE-2017-13089
WWW: https://vuxml.FreeBSD.org/freebsd/09849e71-bb12-11e7-8357-3065ec6f3643.html

krb5-1.15.1_5 is vulnerable:
krb5 -- Multiple vulnerabilities
CVE: CVE-2017-11462
CVE: CVE-2017-11368
WWW: https://vuxml.FreeBSD.org/freebsd/3f3837cc-48fb-4414-aa46-5b1c23c9feae.html

9 problem(s) in the installed packages found.

#6 - 10/30/2017 09:54 AM - Bonnie Follweiler

- Status changed from Resolved to 15

#7 - 10/30/2017 09:54 AM - Bonnie Follweiler

- Status changed from 15 to Ready For Release

- Needs QA changed from Yes to No

- QA Status Test Passes FreeNAS added

- QA Status deleted (Not Tested)

#8 - 10/30/2017 09:56 AM - Dru Lavigne

- Status changed from Ready For Release to Resolved