

Finding: Vulnerable Packages (PKGS-7392)

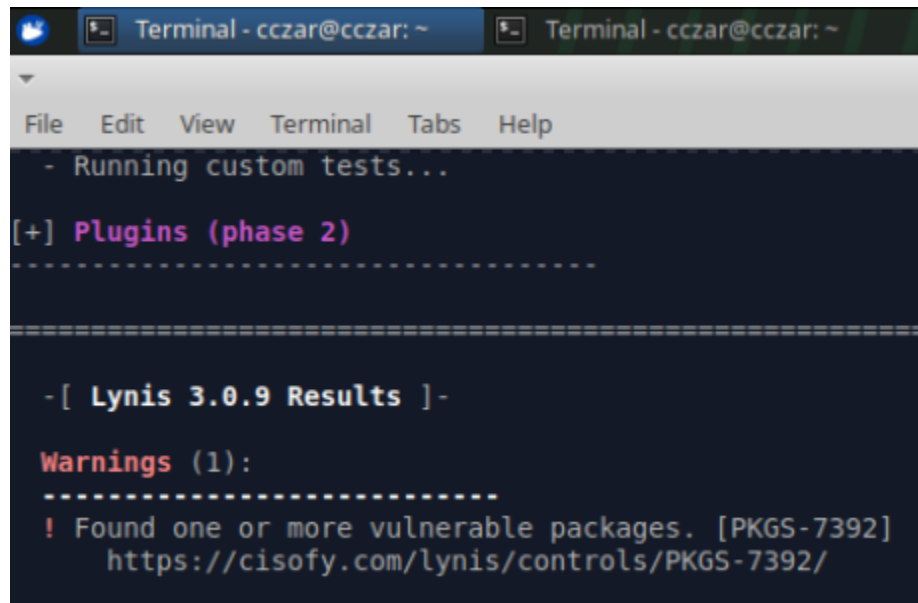
NIST Control Mapping: PR.PS-02 - Software is maintained, replaced, and removed commensurate with risk

Risk: Outdated packages increase the likelihood of compromise, as known vulnerabilities could be exploited.

Severity: High

Remediation: Identify and update all vulnerable packages to the latest stable versions.

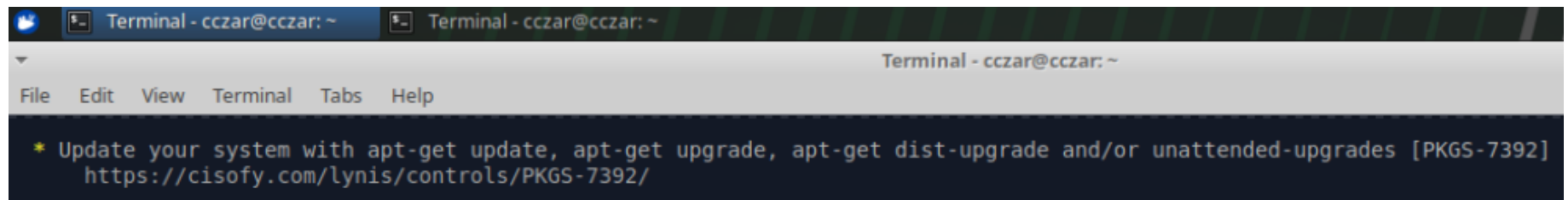
INITIAL LYNIS SCAN RESULT



```
Terminal - cczar@cczar: ~
File Edit View Terminal Tabs Help
- Running custom tests...
[+] Plugins (phase 2)
-----

-[ Lynis 3.0.9 Results ]-

Warnings (1):
-----
! Found one or more vulnerable packages. [PKGS-7392]
  https://cisofy.com/lynis/controls/PKGS-7392/
```



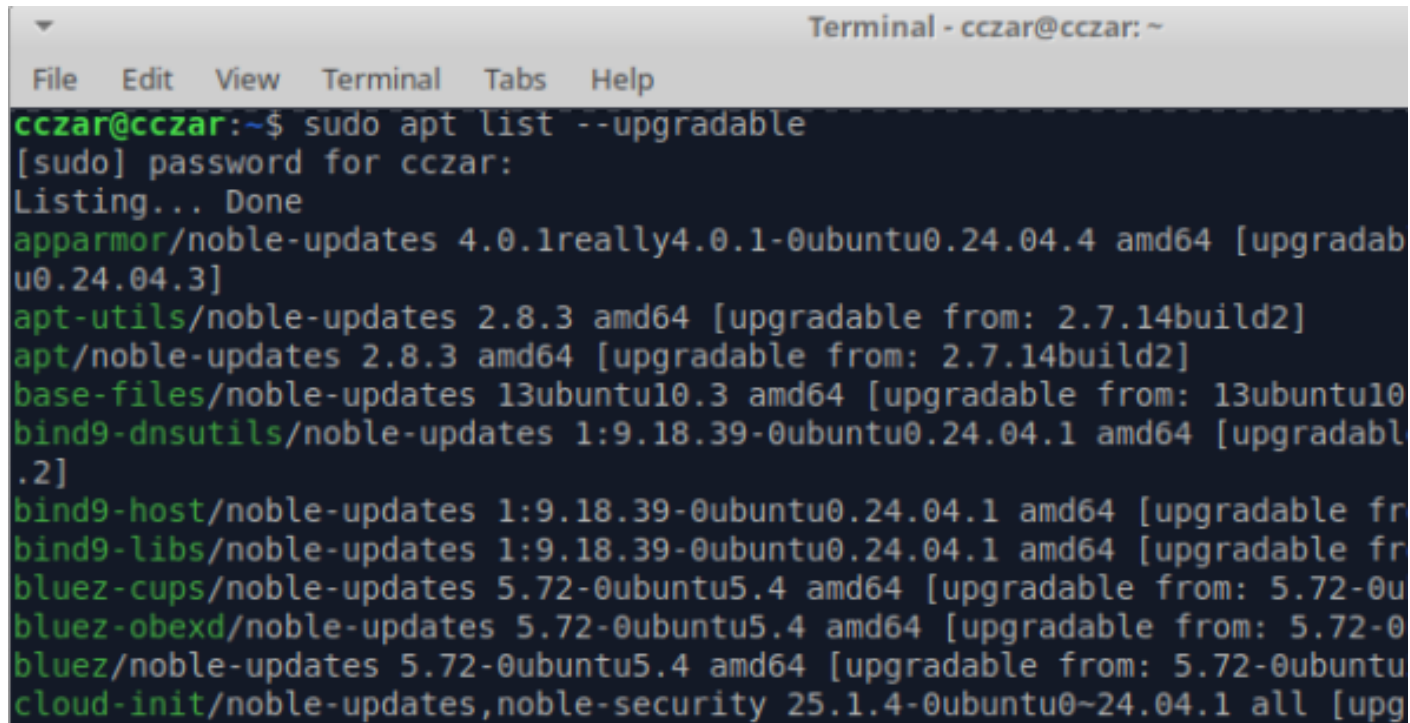
```
Terminal - cczar@cczar: ~
File Edit View Terminal Tabs Help

* Update your system with apt-get update, apt-get upgrade, apt-get dist-upgrade and/or unattended-upgrades [PKGS-7392]
  https://cisofy.com/lynis/controls/PKGS-7392/
```

REMEDIATION PROCESS

1. Searched all vulnerable packages

- A total of 162 packages were found to have upgrades available, including critical system libraries, networking tools, and application utilities. Notable packages included [linux-image-generic](#), [cups](#), [python3.12](#), and [systemd](#).

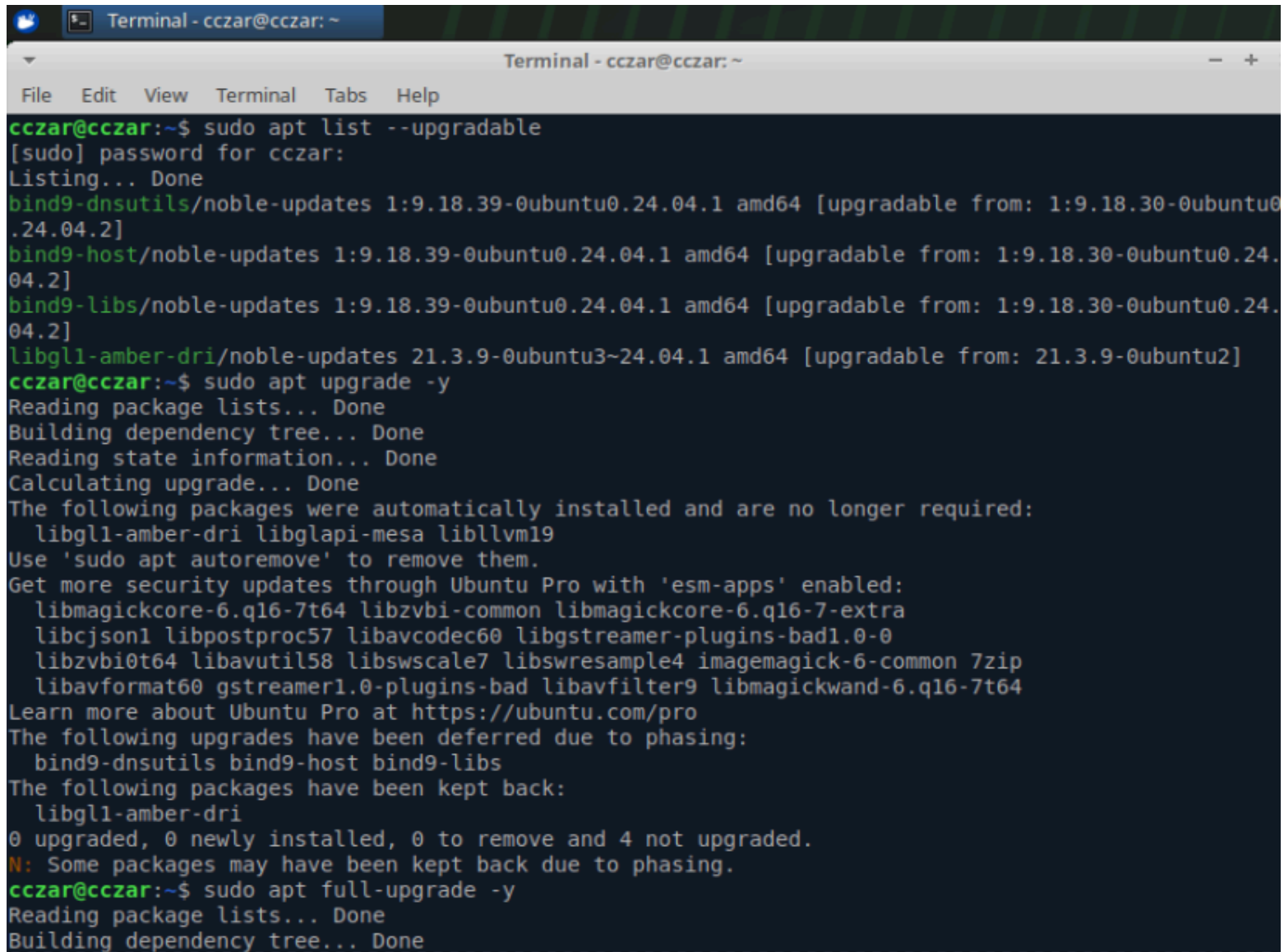


```
Terminal - cczar@cczar: ~
File Edit View Terminal Tabs Help
cczar@cczar:~$ sudo apt list --upgradable
[sudo] password for cczar:
Listing... Done
apparmor/noble-updates 4.0.1really4.0.1-0ubuntu0.24.04.4 amd64 [upgradab
u0.24.04.3]
apt-utils/noble-updates 2.8.3 amd64 [upgradable from: 2.7.14build2]
apt/noble-updates 2.8.3 amd64 [upgradable from: 2.7.14build2]
base-files/noble-updates 13ubuntu10.3 amd64 [upgradable from: 13ubuntu10
bind9-dnsutils/noble-updates 1:9.18.39-0ubuntu0.24.04.1 amd64 [upgradabl
.2]
bind9-host/noble-updates 1:9.18.39-0ubuntu0.24.04.1 amd64 [upgradable fr
bind9-libs/noble-updates 1:9.18.39-0ubuntu0.24.04.1 amd64 [upgradable fr
bluez-cups/noble-updates 5.72-0ubuntu5.4 amd64 [upgradable from: 5.72-0u
bluez-obexd/noble-updates 5.72-0ubuntu5.4 amd64 [upgradable from: 5.72-0
bluez/noble-updates 5.72-0ubuntu5.4 amd64 [upgradable from: 5.72-0ubuntu
cloud-init/noble-updates,noble-security 25.1.4-0ubuntu0~24.04.1 all [upg
```

2. Upgraded all installed packages to the latest security versions

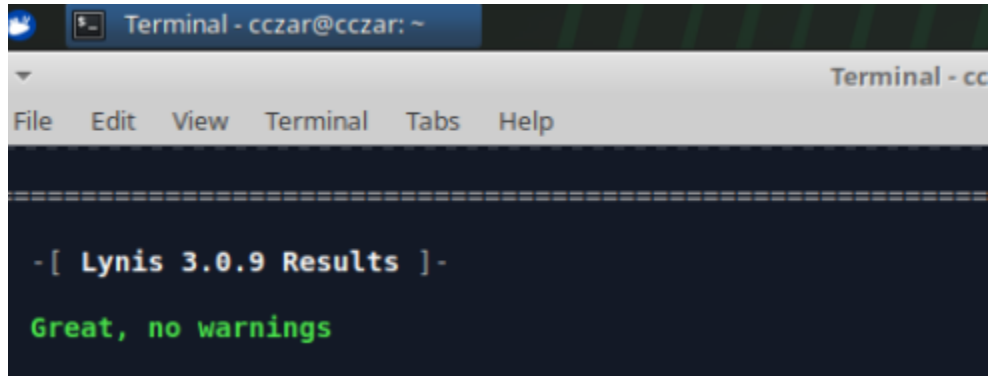
```
Terminal - cczar@cczar: ~
File Edit View Terminal Tabs Help
Get:16 http://us.archive.ubuntu.com/ubuntu noble-backports/restricted amd64 Components [216 B]
Get:17 http://us.archive.ubuntu.com/ubuntu noble-backports/universe amd64 Components [19.2 kB]
Get:18 http://us.archive.ubuntu.com/ubuntu noble-backports/multiverse amd64 Components [212 B]
Fetched 3,904 kB in 2s (1,874 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
162 packages can be upgraded. Run 'apt list --upgradable' to see them.
cczar@cczar:~$ sudo apt update
Hit:1 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:2 http://us.archive.ubuntu.com/ubuntu noble InRelease
Hit:3 http://us.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:4 http://us.archive.ubuntu.com/ubuntu noble-backports InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
162 packages can be upgraded. Run 'apt list --upgradable' to see them.
cczar@cczar:~$ sudo apt upgrade -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
```

3. Verified that all packages were upgraded

A terminal window titled "Terminal - cczar@cczar: ~" with a menu bar (File, Edit, View, Terminal, Tabs, Help). The terminal shows the execution of 'sudo apt list --upgradable' and 'sudo apt upgrade -y'. It lists upgradable packages like bind9-dnsutils, bind9-host, bind9-libs, and libgll-amber-dri. After the upgrade, it lists packages to be removed (libgll-amber-dri, libglapi-mesa, libllvm19) and security updates available (libmagickcore-6.q16-7t64, libzvti-common, etc.). It also shows deferred upgrades (bind9-dnsutils, bind9-host, bind9-libs) and packages kept back (libgll-amber-dri). The final status is "0 upgraded, 0 newly installed, 0 to remove and 4 not upgraded." followed by 'sudo apt full-upgrade -y' which shows package lists and dependency tree updates.

```
cczar@cczar:~$ sudo apt list --upgradable
[sudo] password for cczar:
Listing... Done
bind9-dnsutils/noble-updates 1:9.18.39-0ubuntu0.24.04.1 amd64 [upgradable from: 1:9.18.30-0ubuntu0.24.04.2]
bind9-host/noble-updates 1:9.18.39-0ubuntu0.24.04.1 amd64 [upgradable from: 1:9.18.30-0ubuntu0.24.04.2]
bind9-libs/noble-updates 1:9.18.39-0ubuntu0.24.04.1 amd64 [upgradable from: 1:9.18.30-0ubuntu0.24.04.2]
libgll-amber-dri/noble-updates 21.3.9-0ubuntu3~24.04.1 amd64 [upgradable from: 21.3.9-0ubuntu2]
cczar@cczar:~$ sudo apt upgrade -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  libgll-amber-dri libglapi-mesa libllvm19
Use 'sudo apt autoremove' to remove them.
Get more security updates through Ubuntu Pro with 'esm-apps' enabled:
  libmagickcore-6.q16-7t64 libzvti-common libmagickcore-6.q16-7-extra
  libcjson1 libpostproc57 libavcodec60 libgstreamer-plugins-bad1.0-0
  libzvti0t64 libavutil58 libswscale7 libswresample4 imagemagick-6-common 7zip
  libavformat60 gstreamer1.0-plugins-bad libavfilter9 libmagickwand-6.q16-7t64
Learn more about Ubuntu Pro at https://ubuntu.com/pro
The following upgrades have been deferred due to phasing:
  bind9-dnsutils bind9-host bind9-libs
The following packages have been kept back:
  libgll-amber-dri
0 upgraded, 0 newly installed, 0 to remove and 4 not upgraded.
N: Some packages may have been kept back due to phasing.
cczar@cczar:~$ sudo apt full-upgrade -y
Reading package lists... Done
Building dependency tree... Done
```

LYNIS SCAN RESULT AFTER REMEDIATION

A screenshot of a terminal window titled "Terminal - cczar@cczar: ~". The window has a menu bar with "File", "Edit", "View", "Terminal", "Tabs", and "Help". The terminal content shows a separator line of equals signs, followed by the text "-[Lynis 3.0.9 Results]-" and then "Great, no warnings" in green text.

```
Terminal - cczar@cczar: ~  
File Edit View Terminal Tabs Help  
=====
```

```
-[ Lynis 3.0.9 Results ]-  
Great, no warnings
```