

## Nessus Testing

The instance of Nessus Pro local to Pomona ITS:

<https://nessus.campus.pomona.edu:8834>

Relevant Docs:

[http://info.tenable.com/rs/934-XQB-568/images/NessusPro\\_DS\\_EN\\_v8.pdf](http://info.tenable.com/rs/934-XQB-568/images/NessusPro_DS_EN_v8.pdf)

<https://docs.tenable.com/nessus/Content/Workflow.htm>

<https://docs.tenable.com/nessus/Content/CreateAScan.htm>

<https://docs.tenable.com/nessus/Content/InstallNessusAgentLinux.htm>

<https://www.tenable.com/downloads/nessus-agents>

[https://docs.tenable.com/nessus/Content/Resources/PDF/Nessus\\_7\\_1.pdf](https://docs.tenable.com/nessus/Content/Resources/PDF/Nessus_7_1.pdf)

<https://www.tenable.com/blog/linuxunix-patch-auditing-using-nessus>

Reached out to Nessus to test Nessus Manager:

Thank you for your interest in Nessus® Manager from Tenable Network Security. A Tenable representative will contact you shortly about your evaluation request.

In the meantime, you can learn more about Nessus Manager through these materials:

- Video: [Nessus Manager Deployment Strategies](#)
- Article: [Introducing Nessus Manager and Nessus Cloud](#)
- Video: [Introduction to Nessus Agents](#)
- White Paper: [Understanding Nessus Agents](#)

Sincerely,

The Nessus Manager Team

## Register for tenable.io:

Hello Asya,

We are pleased to offer you an evaluation of the following Tenable.io application(s):

- **Container Security**
- **Vulnerability Management**
- **Web Application Scanning**

Your evaluation is licensed for **60 days** from the date of activation. Once the evaluation period expires, you will need to purchase a subscription to continue your use the Tenable.io application(s) listed above.

[Set your password](#)

### Eval Resources:

To get the most from your evaluation, please make use of the following resources:

- [Product Documentation](#) for more detailed information about features and functionality
- Get access to free [Product Training](#) videos
- The [Tenable Community](#) where you can participate in discussions with peers

For technical issues, please email [eval@tenable.com](mailto:eval@tenable.com) to create a case.

If you have any questions during your trial, or believe you do not have an evaluation underway, please [contact us](#) or your Tenable partner at any time.

<https://cloud.tenable.com/app.html#/dashboards/workbench/vulnerabilities/plugin>

## Install Agents:

```
AsyaShklyer-mac68:~ asaj2017$ sudo /Library/NessusAgent/run/sbin/nessuscli agent link
--host=cloud.tenable.com --port=443
--key=11932b06b801fad4bb291b57dc4e47ef550b72507450655e3ec2cb729555e66a
[info] [agent] HostTag::getUnix: setting TAG value to '9d576462ffeb4a378fdfa4d66aba7c49'
[info] [agent] Successfully linked to cloud.tenable.com:443
```

```
[root@rstudio2 ~]# rpm -ivh /tmp/NessusAgent-7.1.0-es7.x86_64.rpm
warning: /tmp/NessusAgent-7.1.0-es7.x86_64.rpm: Header V4 RSA/SHA1 Signature, key ID
1c0c4a5d: NOKEY
Preparing... ##### [100%]
```

Updating / installing...

1:NessusAgent-7.1.0-es7 ##### [100%]

- First, link this agent to the Nessus Manager with the '/opt/nessus\_agent/sbin/nessuscli agent' command.

Type '/opt/nessus\_agent/sbin/nessuscli agent help' for more info.

- You can start Nessus Agent by typing /bin/systemctl start nessusagent.service

Start Nessus Agent on Linux: /bin/systemctl start nessusagent.service

Link agents to tenable.io:

```
[root@rstudio2 ~]# /opt/nessus_agent/sbin/nessuscli agent link --host=cloud.tenable.com
```

```
--port=443
```

```
--key=11932b06b801fad4bb291b57dc4e47ef550b72507450655e3ec2cb729555e66a
```

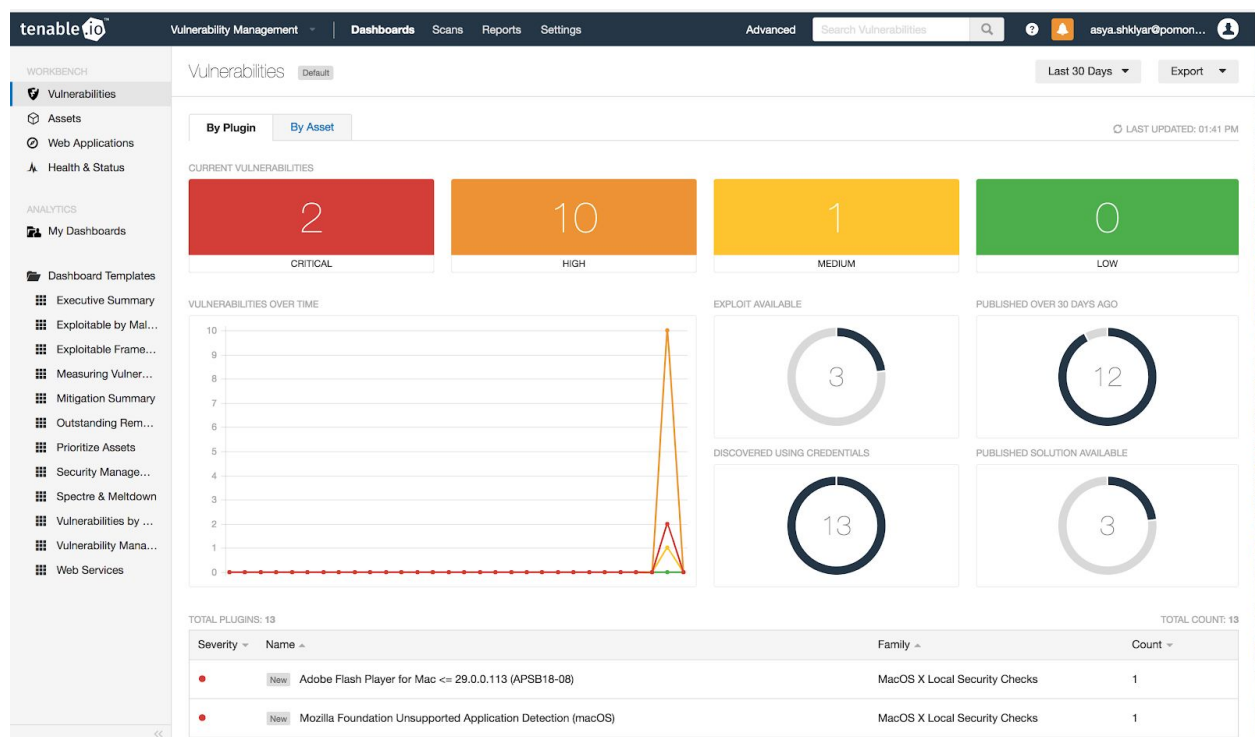
```
[Thu Jun 28 17:31:02 2018][2774.1] _qdb_open:/opt/nessus_agent/var/nessus/plugins-desc.db:
```

```
Invalid table of contents
```

```
[info] [agent] HostTag::getUnix: setting TAG value to '283a5067d8944918a7523a6e2c9cb682'
```

```
[info] [agent] Successfully linked to cloud.tenable.com:443
```

Cole is working with William to get tenable.io (\$8K a year instead of \$2K).



**CRITICAL**

## Adobe Flash Player for Mac <= 29.0.0.113 (APSB18-08)

### Description

The version of Adobe Flash Player installed on the remote macOS or Mac OS X host is equal or prior to version 29.0.0.113. It is therefore affected by multiple vulnerabilities.

### Solution

Upgrade to Adobe Flash Player version 29.0.0.140 or later.

### See Also

<https://helpx.adobe.com/security/products/flash-player/apsb18-08.html>

<http://www.nessus.org/u?0cb17c10>

### Output

```
Path          : /Library/Internet Plug-Ins/Flash Player.plugin
Installed version : 27.0.0.187
Fixed version  : 29.0.0.140
```

Severity ▾	State	Port	Assets
<span style="color: red;">●</span>	New	N/A	<a href="#">asyashklyer-mac68</a>

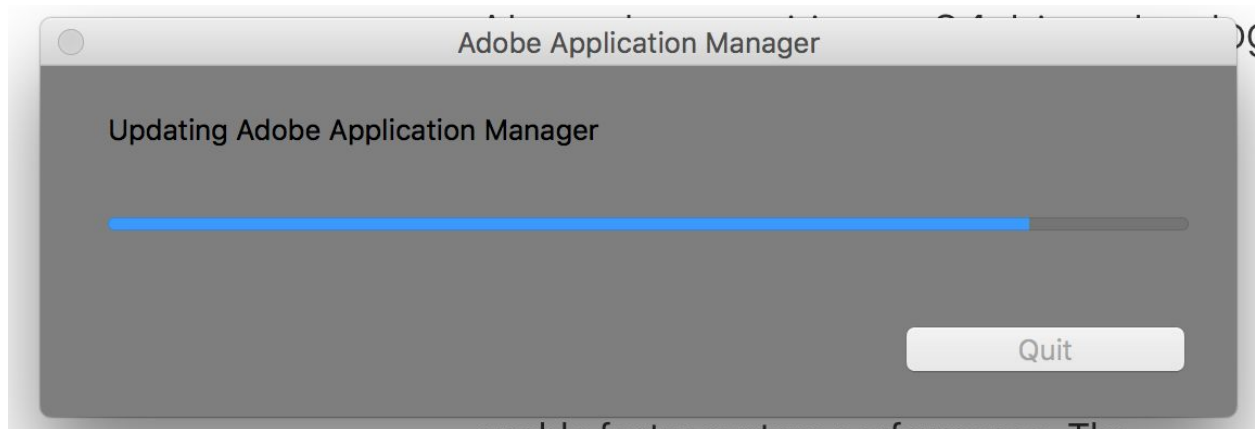


### **"AdobeApplicationManager" is not optimized for your Mac.**

This app needs to be updated by its developer to improve compatibility.

[Learn More...](#)

OK



## 32-bit app compatibility with macOS High Sierra 10.13.4

About the transition to 64-bit technology and how it affects 32-bit apps.

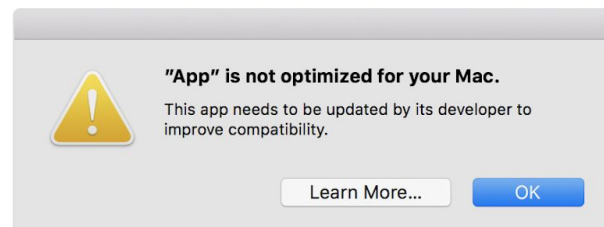
State-of-the-art technology is what makes a Mac a Mac. All modern Macs include powerful 64-bit processors, and macOS runs advanced 64-bit apps, which can access dramatically more memory and enable faster system performance. The technologies that define today's Mac experience—such as [Metal graphics](#)

[acceleration](#)—work only with 64-bit apps. To ensure that the apps you purchase are as advanced as the Mac you run them on, all future Mac software will eventually be required to be 64-bit.

Apple began the transition to 64-bit hardware and software technology for Mac over a decade ago, and is working with developers to transition their apps to 64-bit. At our Worldwide Developers Conference in 2017, Apple informed developers that macOS High Sierra would be the last version of macOS to run 32-bit apps without compromise.

While developers optimize their apps for 64-bit compatibility, Apple is notifying customers when they are using an app based on 32-bit technology. This is done via a one-time alert that appears when you launch a 32-bit app.

Below you will find more information about the alert and what the 64-bit transition means for you.



Security updates available for Flash Player | APSB18-08

Bulletin ID	Date Published	Priority
APSB18-08	April 10, 2018	2

## Version Information

You have version  
30,0,0,113 installed

**CRITICAL** Mozilla Foundation Unsupported Application Detection (macOS)

**Description**

According to its version, there is at least one unsupported Mozilla application (Firefox and/or Thunderbird) installed on the remote host. This version of the software is no longer actively maintained.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

**Solution**

Upgrade to a version that is currently supported.

**See Also**

<https://www.mozilla.org/en-US/firefox/organizations/faq/>  
<https://www.mozilla.org/en-US/security/known-vulnerabilities/>  
<https://www.mozilla.org/en-US/firefox/new/>  
<https://www.mozilla.org/en-US/thunderbird/>

**Output**

<div>Product : Firefox ESR Path : /Applications/Firefox.app Installed version : 52.5.2 Latest version : 52.8.0 EOL URL : <a href="https://www.mozilla.org/en-US/security/known-vulnerabilities/firefox-esr/">https://www.mozilla.org/en-US/security/known-vulnerabilities/firefox-esr/</a></div>			
Severity ▾	State	Port	Assets
<div>●</div>	<div>New</div>	<div>N/A</div>	<div><a href="#">asyashkiyer-mac68</a></div>



# Firefox ESR

**52.5.2 (64-bit)** [What's new](#)

Restart Firefox to Update

You are currently on the **esr** update channel.

Firefox is designed by [Mozilla](#), a [global community](#) working together to keep the Web open, public and accessible to all.

Want to help? [Make a donation](#) or [get involved!](#)



## Firefox Quantum

**61.0 (64-bit)** [What's new](#)

Firefox is up to date

Firefox is designed by [Mozilla](#), a [global community](#) working together to keep the Web open, public and accessible to all.

Want to help? [Make a donation](#) or [get involved!](#)

[Licensing Information](#)

[End-User Rights](#)

[Privacy Policy](#)

Firefox and the Firefox logos are trademarks of the Mozilla Foundation.



Assets

0

Notes

1

History

1

#### Scan Notes

**Agent unscanned**

Scan not started for agent 'rstudio2.campus.pomona.edu' at 10.16.8.247. Agent with plugin set: null last connected: null and last scanned null.

## Scan Details

Name: Linux Scan

Status: Completed

Policy: Advanced Agent Scan

Start: June 28 at 5:33 PM

End: June 28 at 8:33 PM

Elapsed: 3 hours

## Agent Details

Groups: [Linux Servers](#)

Reported: 0 of 1

Scan Window

1 day



Agents must report within this timeframe to be visible in scan results.

Scanned a Mac (my own) and a Linux (RStudio2)

Mac found 2 criticals.

Adobe version seems to be a bug because it says install above version 29 but I have v30 installed. Will need to submit a ticket with support.

Firefox was updated. Re-running the scan.

Linux scan returned zero information, possibly because of a 3 hours scanning window? Increased to 1 day. Re-running.

These are the details of trying to start the Linux Agent:

```
[asaj2017@rstudio2 ~]$ /bin/systemctl start nessusagent.service
```

**==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====**

Authentication is required to manage system services or units.

Multiple identities can be used for authentication:

1. Patrick Flannery (pat)
2. Linux Admin,18506,Pomona ITB (jbsadmin)

Choose identity to authenticate as (1-2):

```
[root@rstudio2 ~]# /bin/systemctl start nessusagent.service
```

Added asaj2017 to visudo

```
[root@rstudio2 rules.d]# cat /etc/group
```

root:x:0:

bin:x:1:

daemon:x:2:

sys:x:3:

adm:x:4:

tty:x:5:

disk:x:6:

```
lp:x:7:
mem:x:8:
kmem:x:9:
wheel:x:10:pat,jbsadmin
```

```
[root@rstudio2 ~]# cd /etc/polkit-1/
[root@rstudio2 polkit-1]# ls
localauthority localauthority.conf.d rules.d
[root@rstudio2 polkit-1]# cd rules.d/
```

```
[root@rstudio2 rules.d]# cat 50-default.rules
/* -*- mode: js; js-indent-level: 4; indent-tabs-mode: nil -*- */
```

```
// DO NOT EDIT THIS FILE, it will be overwritten on update
//
// Default rules for polkit
//
// See the polkit(8) man page for more information
// about configuring polkit.
```

```
polkit.addAdminRule(function(action, subject) {
    return ["unix-group:wheel"];
});
```

This is a screenshot of what happens if you forgot to start the Nessus Agent on Linux:

Agent Group / Linux Servers [Back to Agent Groups](#) [Add Members](#)

Members									
Settings Permissions									
<input type="checkbox"/>	Name ^	Status	IP Address	Platform	Groups	Version	Last Plugin Update	Last Scanned	
<input type="checkbox"/>	rstudio2.campus.pomona.edu	● Offline	10.16.8.247	Linux (es7-x86-...	Linux Servers	N/A	N/A	N/A	✕

The rescan of the Mac shows that Firefox is fixed.

Severity ▾	Name ▲
●	New Adobe Flash Player for Mac <= 29.0.0.113 (APSB18-08)
●	New Adobe Flash Player for Mac <= 28.0.0.126 (APSB18-01)
●	New Adobe Flash Player for Mac <= 28.0.0.137 Use-after-free Remote Code Execution (APSA18-01) (APSB1...
●	New Adobe Flash Player for Mac <= 28.0.0.161 (APSB18-05)
●	New Adobe Flash Player for Mac <= 29.0.0.140 (APSB18-16)
●	New Adobe Flash Player for Mac <= 29.0.0.171 <b>Plugin ID: 105176</b>
●	New Adobe Flash Player for Mac <= 27.0.0.187 (APSB17-42)

## Vulnerabilities / Critical

[◀ Back to Workbench](#)

TOTAL PLUGINS: 3

Severity ▾	Name ▲
●	New Adobe Flash Player for Mac <= 29.0.0.113 (APSB18-08)
●	New CentOS 7 : kernel (CESA-2017:1842) (Stack Clash)
●	New CentOS 7 : kernel (CESA-2017:2930)

CRITICAL

## CentOS 7 : kernel (CESA-2017:1842) (Stack Clash)

### Description

An update for kernel is now available for Red Hat Enterprise Linux 7.

Red Hat Product Security has rated this update as having a security impact of Important. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) in the References section.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fix(es) :

\* An use-after-free flaw was found in the Linux kernel which enables a race condition in the L2TPv3 IP Encapsulation feature. A local user could use this flaw to escalate their privileges or crash the system.

(CVE-2016-10200, Important)

\* A flaw was found that can be triggered in keyring\_search\_iterator in keyring.c if type->match is NULL. A local user could use this flaw to crash the system or, potentially, escalate their privileges.

(CVE-2017-2647, Important)

\* It was found that the NFSv4 server in the Linux kernel did not properly validate layout type when processing NFSv4 pNFS LAYOUTGET and GETDEVICEINFO operands. A remote attacker could use this flaw to soft-lockup the system and thus cause denial of service.

(CVE-2017-8797, Important)

This update also fixes multiple Moderate and Low impact security issues :

\* CVE-2015-8839, CVE-2015-8970, CVE-2016-9576, CVE-2016-7042, CVE-2016-7097, CVE-2016-8645, CVE-2016-9576, CVE-2016-9588, CVE-2016-9806, CVE-2016-10088, CVE-2016-10147, CVE-2017-2596, CVE-2017-2671, CVE-2017-5970, CVE-2017-6001, CVE-2017-6951, CVE-2017-7187, CVE-2017-7616, CVE-2017-7889, CVE-2017-8890, CVE-2017-9074, CVE-2017-8890, CVE-2017-9075, CVE-2017-8890, CVE-2017-9076, CVE-2017-8890, CVE-2017-9077, CVE-2017-9242, CVE-2014-7970, CVE-2014-7975, CVE-2016-6213, CVE-2016-9604, CVE-2016-9685

## Output

```
Remote package installed : kernel-3.10.0-514.26.2.el7
Should be                : kernel-3.10.0-693.el7

Remote package installed : kernel-headers-3.10.0-514.26.2.el7
Should be                : kernel-headers-3.10.0-693.el7

Remote package installed : kernel-tools-3.10.0-514.26.2.el7
Should be                : kernel-tools-3.10.0-693.el7

Remote package installed : kernel-tools-libs-3.10.0-514.26.2.el7
Should be                : kernel-tools-libs-3.10.0-693.el7

Remote package installed : python-perf-3.10.0-514.26.2.el7
Should be                : python-perf-3.10.0-693.el7
```

Severity ▾	State	Port	Assets
	New	N/A	<a href="https://rstudio2.campus.pomona.edu">rstudio2.campus.pomona.edu</a>

CRITICAL

## CentOS 7 : kernel (CESA-2017:2930)

### Description

An update for kernel is now available for Red Hat Enterprise Linux 7.

Red Hat Product Security has rated this update as having a security impact of Important. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) in the References section.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fix(es) :

\* Out-of-bounds kernel heap access vulnerability was found in xfrm, kernel's IP framework for transforming packets. An error dealing with netlink messages from an unprivileged user leads to arbitrary read/write and privilege escalation. (CVE-2017-7184, Important)

\* A race condition issue leading to a use-after-free flaw was found in the way the raw packet sockets are implemented in the Linux kernel networking subsystem handling synchronization. A local user able to open a raw packet socket (requires the CAP\_NET\_RAW capability) could use this flaw to elevate their privileges on the system.  
(CVE-2017-1000111, Important)

\* An exploitable memory corruption flaw was found in the Linux kernel.  
The append path can be erroneously switched from UFO to non-UFO in ip\_ufo\_append\_data() when building an UFO packet with MSG\_MORE option.  
If unprivileged user namespaces are available, this flaw can be exploited to gain root privileges. (CVE-2017-1000112, Important)

\* A flaw was found in the Linux networking subsystem where a local attacker with CAP\_NET\_ADMIN capabilities could cause an out-of-bounds memory access by creating a smaller-than-expected ICMP header and sending to its destination via sendto(). (CVE-2016-8399, Moderate)

\* Kernel memory corruption due to a buffer overflow was found in brcmf\_cfg80211\_mgmt\_tx() function in Linux kernels from v3.9-rc1 to v4.13-rc1. The vulnerability can be triggered by sending a crafted NL80211\_CMD\_FRAME packet via netlink. This flaw is unlikely to be triggered remotely as certain userspace code is needed for this. An unprivileged local user could use this flaw to induce kernel memory corruption on the system, leading to a crash. Due to the nature of the flaw, privilege escalation cannot be fully ruled out, although it is unlikely. (CVE-2017-7541, Moderate)

\* An integer overflow vulnerability in ip6\_find\_1stfragopt() function was found. A local attacker that has privileges (of CAP\_NET\_RAW) to open raw socket can cause an infinite loop inside the ip6\_find\_1stfragopt() function. (CVE-2017-7542, Moderate)



## Output


```
Remote package installed : kernel-3.10.0-514.26.2.el7
Should be                : kernel-3.10.0-693.5.2.el7

Remote package installed : kernel-headers-3.10.0-514.26.2.el7
Should be                : kernel-headers-3.10.0-693.5.2.el7

Remote package installed : kernel-tools-3.10.0-514.26.2.el7
Should be                : kernel-tools-3.10.0-693.5.2.el7

Remote package installed : kernel-tools-libs-3.10.0-514.26.2.el7
Should be                : kernel-tools-libs-3.10.0-693.5.2.el7

Remote package installed : python-perf-3.10.0-514.26.2.el7
Should be                : python-perf-3.10.0-693.5.2.el7
```

Severity ▼	State	Port	Assets
	New	N/A	<a href="https://rstudio2.campus.pomona.edu">rstudio2.campus.pomona.edu</a>