Enabling SELinux

Devconf 2018

Lukas Vrabec
lvrabec@redhat.com

Agenda

1. Disabled SELinux - What does it mean for me?
2. Infrastructure introduction
3. How to enable SELinux ?
4. Troubleshooting
5. Enforced SELinux
6. Deployment

Meltdown & Spectre vs. SELinux

Unfortunately SELinux cannot mitigate damage caused by recently disclosed vulnerabilities Meltdown and Spectre.

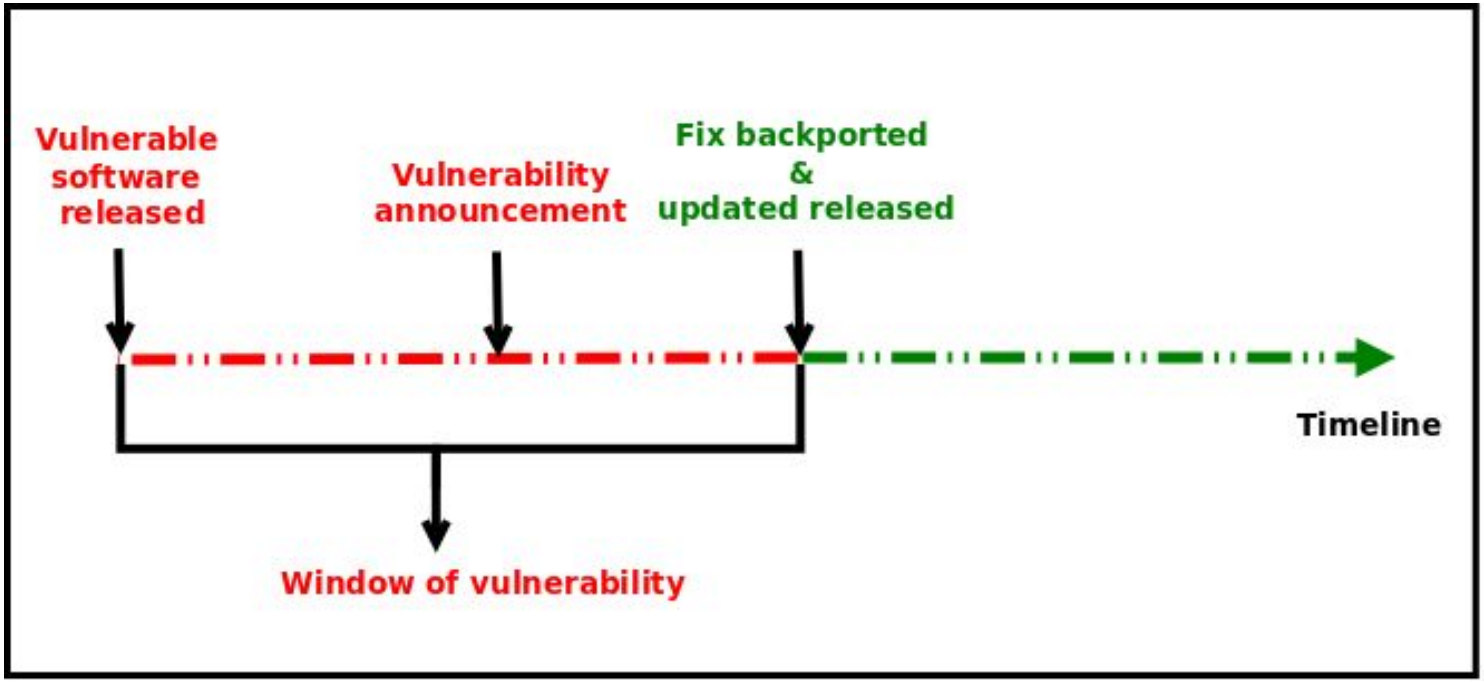
Default state of SELinux on Fedora and Red Hat Enterprise Linux

- SELinux is in Enforcing state by default on both Fedora and RHEL
- Unfortunately it’s common practise to disable SELinux, configure a server and then try to enable SELinux again

Disabled SELinux

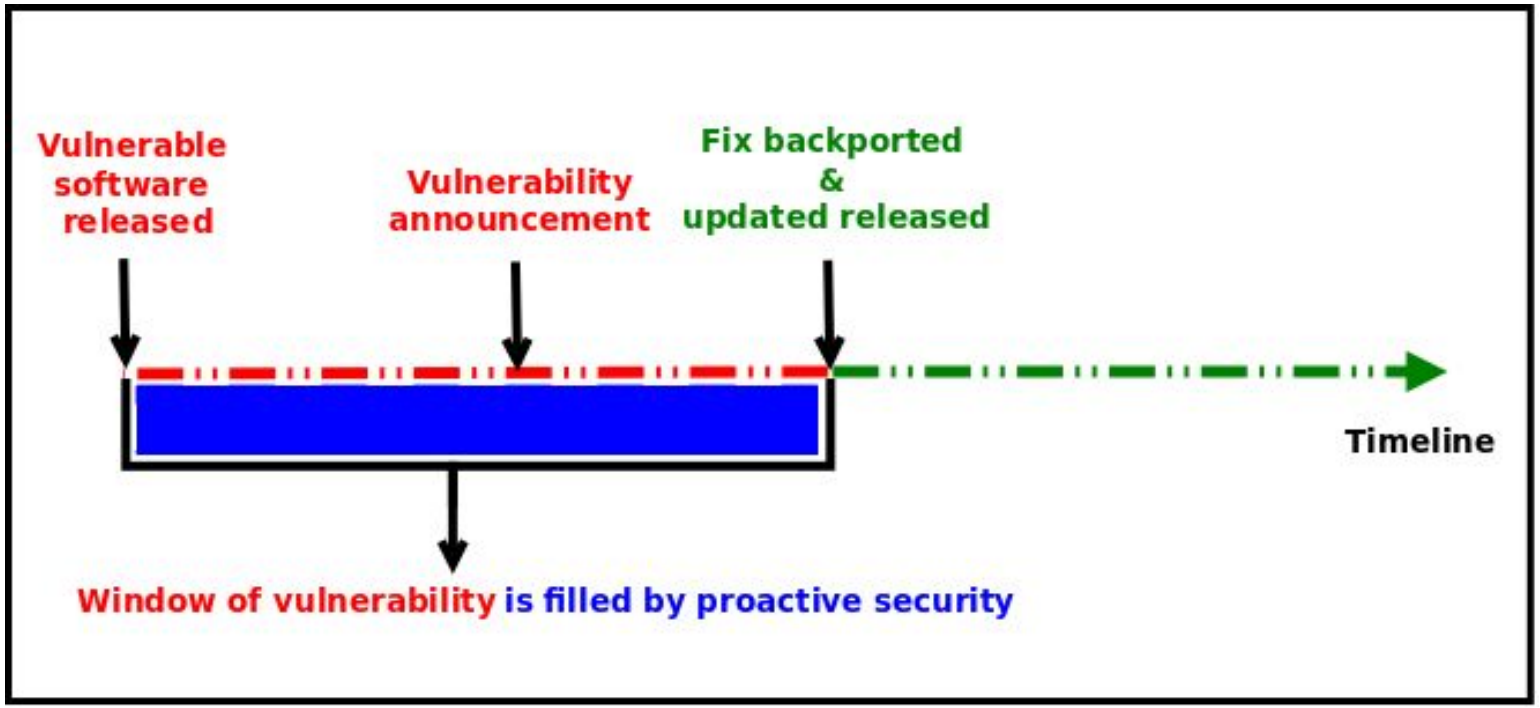
What does it mean for me?

MY SYSTEMS **ARE NOT PROTECTED** DURING THE WINDOW OF VULNERABILITY!


Vulnerable
software
released
Vulnerability
announcement
Fix backported
&
updated released
Timeline
Window of vulnerability

PROACTIVE SECURITY HELPS TO **PROTECT** YOUR SYSTEM DURING THE WINDOW OF VULNERABILITY!

SECURITY ENHANCED LINUX IS A SECURITY MECHANISM BRINGING PROACTIVE SECURITY FOR YOUR SYSTEM


Vulnerable software released
Vulnerability announcement
Fix backported & updated released
Timeline
Window of vulnerability is filled by proactive security

Infrastructure Introduction

Infrastructure

- Server
  - Disabled SELinux
  - Web server listening on 80/7070 tcp ports
  - Cockpit web server

This is replicated on Fedora 28, RHEL-6.10 and RHEL-7.5

How to Enable SELinux?

getenforce
Disabled

Enabling SELinux

- Modify /etc/selinux/config
  - SELINUX=disabled
  - SELINUX=permissive
- # fixfiles onboot && reboot

getenforce
Permissive

Move web page content from homedir to /var/www/html

```
# mv ~/my_web/* /var/www/html/
```

Let’s check our web content!

- http://rhel7.devconf.local Working…
- http://rhel7.devconf.local:7070 Working...

It looks like we are done...
we can switch to Enforcing mode

setenforce 1

- http://rhel7.devconf.local Not Working…
- http://rhel7.devconf.local:7070 Not Working...

Troubleshooting

Where can I find SELinux denials?

Where can I find SELinux denials?

- Desktop
  - SEAlert
- Server
  - Console / ausearch
  - Cockpit

SELinux Alert Browser

SELinux has detected a problem.

Would you like to receive alerts? Yes No

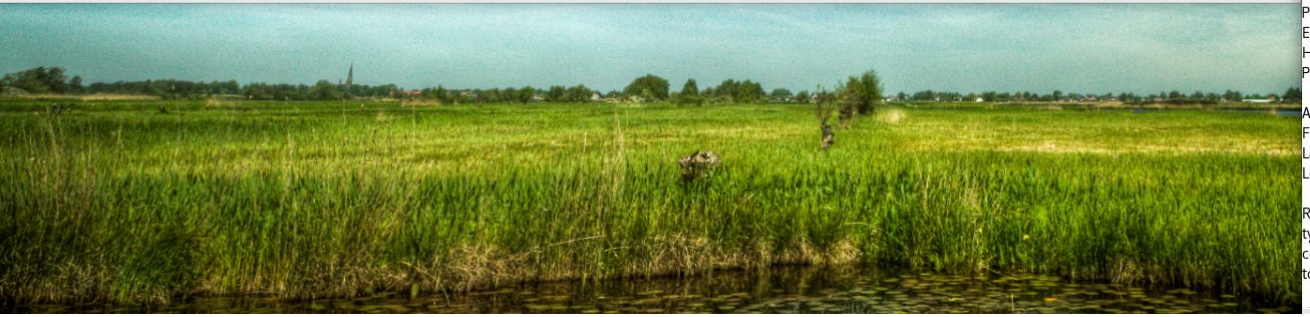
The source process: ssh
Attempted this access: name_connect
On this tcp_socket: port 443

Tue Nov 7, 2017 10:35 CET

Troubleshoot | Notify Admin | Details | Ignore | Delete

If you were trying to...	Then this is the solution.	
If you want to allow system to run with NIS	You must tell SELinux about this by enabling the 'nis_enabled' boolean. setsebool -P nis_enabled 1	Plugin Details
If you believe that ssh should be allowed name_connect access on the port 443 tcp_socket by default.	You should report this as a bug. You can generate a local policy module to allow this access. Allow this access for now by executing: # ausearch -c 'ssh' --raw | audit2allow -M my-ssh # semodule -X 300 -i my-ssh.pp	Plugin Details Report Bug

Previous | Alert 23 of 36 | Next | List All Alerts



SETroubleshoot Details Window

SELinux is preventing ssh from name_connect access on the tcp_socket port 443.

***** Plugin catchall_boolean (89.3 confidence) suggests ******************

If you want to allow system to run with NIS
Then you must tell SELinux about this by enabling the 'nis_enabled' boolean.

Do
setsebool -P nis_enabled 1

***** Plugin catchall (11.6 confidence) suggests **************************

If you believe that ssh should be allowed name_connect access on the port 443 tcp_socket by default.
Then you should report this as a bug.
You can generate a local policy module to allow this access.
Do
allow this access for now by executing:
ausearch -c 'ssh' --raw | audit2allow -M my-ssh
semodule -X 300 -i my-ssh.pp

Additional Information:

Source Context	staff_u:staff_r:ssh_t:s0:c0.c1023
Target Context	system_u:object_r:http_port_t:s0
Target Objects	port 443 [tcp_socket]
Source	ssh
Source Path	ssh
Port	443
Host	lvrabec-workstation
Source RPM Packages	
Target RPM Packages	
Policy RPM	selinux-policy-3.13.1-260.15.fc26.noarch
Selinux Enabled	True
Policy Type	targeted
Enforcing Mode	Enforcing
Host Name	lvrabec-workstation
Platform	Linux lvrabec-workstation 4.13.10-200.fc26.x86_64 #1 SMP Fri Oct 27 15:34:40 UTC 2017 x86_64 x86_64
Alert Count	53
First Seen	2017-11-07 08:57:35 CET
Last Seen	2017-11-07 10:35:27 CET
Local ID	129d8f59-34d8-45f4-a67b-8dff456bd57b

Raw Audit Messages
type=AVC msg=audit(1510047327.231:2770): avc: denied { name_connect } for pid=16032 comm="ssh" dest=443 scontext=staff_u:staff_r:ssh_t:s0:c0.c1023 tcontext=system_u:object_r:http_port_t:s0 tclass=tcp_socket permissive=0

Console / ausearch

ausearch -m AVC -ts today

…..

ausearch -m AVC -ts today | audit2allow

…..

Cockpit

- Cockpit provides SELinux plugin for troubleshooting SELinux issues
- SEAlert for servers.

restorecon

- Tool for restoring labels on your system
  - Checks for Labels Defined in SELinux db and if given object has a different label, restorecon will restore the default one
- # restorecon -Rv /var/www/html/

Tcp port 7070 is not default port for httpd!

semanage port

- Tools for handling SELinux labels on ports, you can:
  - Add SELinux labels for ports
  - Modify SELinux labels for ports
- # semanage port -l
- # semanage port -a -t http_port_t -p tcp 7070

/var/www_new/html is not default path for webpage content!

semanage fcontext

- Tools for handling SELinux labels on objects, you can:
  - Add SELinux labels for files/dirs/sym_links/sockets
  - Modify SELinux labels for files/dirs/sym_links/sockets
- # semanage fcontext -l
- # semanage fcontext -a -t httpd_sys_content_t /var/www_new(/.*)?
- # restorecon -Rv /var/www_new

Enabling SELinux

- Modify /etc/selinux/config
  - SELINUX=permissive
  - SELINUX=enforcing
- # reboot

getenforce
Enforcing

Deploying

We have properly configured SELinux on one system, what about others?

Let’s use ansible to deploy the same configuration to the rest of the servers!

I'll use the following Ansible role:
https://github.com/linux-system-roles/selinux

Expected functionality

- Set enforcing/permissive
- restorecon portions of filesystem tree
- Set/Get Booleans
- Set/Get file contexts
- Manage logins
- Manage ports

```yaml
---
- hosts: all
  become: true
  become_method: sudo
  become_user: root
  vars:
    SELinux_type: targeted
    SELinux_mode: enforcing
    SELinux_change_running: 1
    SELinux_booleans:
      - { name: 'samba_enable_home_dirs', state: 'on' }
      - { name: 'ssh_sysadm_login', state: 'on', persistent: 'yes' }
    SELinux_file_contexts:
      - { target: '/tmp/test_dir(/.*)?', setype: 'user_home_dir_t', ftype: 'd' }
    SELinux_restore_dirs:
      - /tmp/test_dir
    SELinux_ports:
      - { ports: '22100', proto: 'tcp', setype: 'ssh_port_t', state: 'present' }
    SELinux_logins:
      - { login: 'sar-user', seuser: 'staff_u', serange: 's0-s0:c0.c1023', state: 'present' }

  # prepare prerequisites which is used in this playbook
  pre_tasks:
    - name: Creates directory
      file:
        path: /tmp/test_dir
        state: directory
    - name: Add a System Api Roles SELinux User
      user:
        comment: System Api Roles SELinux User
        name: sar-user

  roles:
    - selinux
```

How to do it:

- # dnf install ansible-python3
- # ansible-galaxy install linux-system-roles.selinux

Inventory file:

- $ cat /etc/ansible/hosts
  - rhel6.devconf.local
  - rhel7-2.devconf.local
  - fedora.devconf.local

- # ansible -m ping all -u root
- # ansible -a getenforce all -u root
- # ansible-playbook -i /etc/ansible/hosts setup-selinux.yml -u root

```
---
- hosts: all
  become: true
  become_user: root

  pre_tasks:
  - name: Enable SELinux and reboot when SELinux is disabled
    block:
      - name: Enable SELinux
        selinux:
          policy: targeted
          state: permissive
      - name: Reboot the machine
        shell: sleep 2 && shutdown -r now
        async: 1
        poll: 0
      - name: Wait for machine to come back
        wait_for:
          port: 22
          host: "{{ ansible_default_ipv4.address }}"
          delay: 5
          timeout: 300
        delegate_to: localhost
        become: false
      - name: Gather new facts
        setup:
      - debug:
          msg: "SELinux status = {{ ansible_selinux.status }}"
    when: ansible_selinux.status == "disabled"

  vars_files:
    - my-setup.yml

  roles:
    - linux-system-roles.selinux
```

```
---
SELinux_type: targeted
SELinux_mode: enforcing
SELinux_change_running: 1
SELinux_file_contexts:
  - { target: '/var/www_new(/.*)?', setype: 'httpd_sys_content_t', ftype: 'd' }
SELinux_restore_dirs:
  - /var/www/html
  - /var/www_new/
SELinux_ports:
  - { ports: '7070', proto: 'tcp', setype: 'http_port_t', state: 'present' }
```

- **$ ansible -a getenforce all -u root**

rhel7.devconf.local | SUCCESS | rc=0 >>

Enforcing

fedora.devconf.local | SUCCESS | rc=0 >>

Enforcing

rhel6.devconf.local | SUCCESS | rc=0 >>

Enforcing

QUESTIONS?

Miroslav Grepl's blog	https://mgrepl.wordpress.com/
Paul Moore's blog	http://www.paul-moore.com/
Petr Lautrbach's blog	https://plautrba.fedorapeople.org/
Lukas Vrabec's blog	https://lukas-vrabec.com/
Dan Walsh's blog	http://danwalsh.livejournal.com/

THANK YOU