1.5.3 Ensure address space layout randomization (ASLR) is enabled (Scored)

Profile Applicability

```
Level 1 - Server
Level 1 - Workstation
```

Description

Address space layout randomization (ASLR) is an exploit mitigation technique which randomly arranges the address space of key data areas of a process.

Rationale

Randomly placing virtual memory regions will make it difficult to write memory page exploits as the memory placement will be consistently shifting.

Audit

Run the following command and verify output matches:

```
# sysctl kernel.randomize_va_space
kernel.randomize_va_space = 2
```

Remediation

Set the following parameter in the /etc/sysctl.conf file:

```
kernel.randomize_va_space = 2
```

Run the following command to set the active kernel parameter:

```
# sysctl -w kernel.randomize_va_space=2
```

From:
https://secscan.acron.pl/ - **SecScan**

Permanent link:
https://secscan.acron.pl/centos7/1/5/3

Last update: **2017/05/05 22:40**