

## 3.2.1 Ensure source routed packets are not accepted (Scored)

### Profile Applicability

Level 1 - Server  
Level 1 - Workstation

### Description

In networking, source routing allows a sender to partially or fully specify the route packets take through a network. In contrast, non-source routed packets travel a path determined by routers in the network. In some cases, systems may not be routable or reachable from some locations (e.g. private addresses vs. Internet routable), and so source routed packets would need to be used.

### Rationale

Setting `net.ipv4.conf.all.accept_source_route` and `net.ipv4.conf.default.accept_source_route` to 0 disables the system from accepting source routed packets. Assume this system was capable of routing packets to Internet routable addresses on one interface and private addresses on another interface. Assume that the private addresses were not routable to the Internet routable addresses and vice versa. Under normal routing circumstances, an attacker from the Internet routable addresses could not use the system as a way to reach the private address systems. If, however, source routed packets were allowed, they could be used to gain access to the private address systems as the route could be specified, rather than rely on routing protocols that did not allow this routing.

### Audit

Run the following command and verify output matches:

```
# sysctl net.ipv4.conf.all.accept_source_route
net.ipv4.conf.all.accept_source_route = 0
# sysctl net.ipv4.conf.default.accept_source_route
net.ipv4.conf.default.accept_source_route = 0
```

### Remediation

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

```
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.default.accept_source_route = 0
```

Run the following commands to set the active kernel parameters:

```
# sysctl -w net.ipv4.conf.all.accept_source_route=0
# sysctl -w net.ipv4.conf.default.accept_source_route=0
# sysctl -w net.ipv4.route.flush=1
```

From:

<https://secscan.acron.pl/> - **SecScan**

Permanent link:

<https://secscan.acron.pl/ubuntu1604/3/2/1>

Last update: **2017/05/03 15:01**

