Article Number: 0001085
Title: Dirty COW Vulnerability – CVE-2016-519

Summary

Skybox Appliances based on CentOS 5, 6, and 7, are vulnerable to Dirty COW vulnerability - CVE–2016–5195. This article provides information on testing the appliance to determine whether it is vulnerable as well information on patching vulnerable systems.
Important to mention, that this vulnerability becomes less critical for Skybox Appliances, as far as all appliance users (root and skyboxview) are administrators in a varying degree.
Please doublecheck that there were no additional users defined, and if they were – deactivate them.

Background

A race condition was found in the way Linux kernel's memory subsystem handled breakage of the read only private mappings COW situation on write access. An unprivileged local user could use this flaw to gain write access to otherwise read only memory mappings and thus increase their privileges on the system.
Extra information link.

Vulnerable Skybox Products

Skybox Appliances based on CentOS 5, 6, and 7.

Testing for vulnerable appliances

Some versions of CentOS can use the script (`rh-cve-2016-5195_1.sh`) provided by RedHat for RHEL to test your server's vulnerability.
To do this, first download the script:

```
wget https://access.redhat.com/sites/default/files/rh-cve-2016-5195_2.sh
```

Then run it with bash:

```
bash rh-cve-2016-5195_1.sh
```

If you're vulnerable, you'll see output like this:

```
Output
Your kernel is 3.10.0-327.36.1.el7.x86_64 which IS vulnerable.
Red Hat recommends that you update your kernel. Alternatively, you can apply
partial mitigation described at
https://access.redhat.com/security/vulnerabilities/2706661.
```


© 2015 Skybox Security, Inc. All rights reserved.
Proprietary & Confidential

Patching the Vulnerability – ***must be Root user / reboot required after implementation***

CentOS-6 package:

```
wget http://downloads.skyboxsecurity.com/files/Other/DirtyCowFix/kernel-2.6.32-642.6.2.el6.x86_64.rpm

Checksum - b5880cb6606887ce75a2e0d8690e94d2
```

CentOS-7 package:

```
wget http://downloads.skyboxsecurity.com/files/Other/DirtyCowFix/kernel-3.10.0-327.36.3.el7.x86_64.rpm

Checksum - 90ce09ee1c06593a6073fecf32fdf9d6
```

Right now, we're still waiting on a fix for CentOS 5. In the interim, you can use this workaround from the Red Hat bug tracker.

© 2015 Skybox Security, Inc. All rights reserved.
Proprietary & Confidential