

# HPE Software Security Update

## HPE Propel Propel Update for Linux Kernel Vulnerability (CVE-2016-4997)

---

### Document management:

Date	Version	Change
4-Oct-2016	1.0	Initial Release

### Summary:

From <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4997>:

The compat IPT\_SO\_SET\_REPLACE and IP6T\_SO\_SET\_REPLACE setsockopt implementations in the netfilter subsystem in the Linux kernel before 4.6.3 allow local users to gain privileges or cause a denial of service (memory corruption) by leveraging in-container root access to provide a crafted offset value that triggers an unintended decrement.

### Topic

Find out more about CVE-2016-4997 from the [MITRE CVE dictionary](#).

*HPE has investigated the CVE-2016-4997 vulnerability in relation to HPE Propel. This document provides required actions that must be performed to mitigate this vulnerability.*

### Affected Releases: 1.01, 1.11, 2.01, 2.10, 2.20

**ACTION:** Review all details in instructions provided in this paper to address the vulnerability. HPE SW recommend to address this information as soon as possible.

## Response

### Impact on HPE Propel

All versions of the HPE Propel OVA ship with a kernel that is vulnerable to the exploits described in 2016-4997.

### Mitigation Actions

To update the kernel the HPE Propel VM, execute:

```
# yum -y update kernel
# /sbin/shutdown -r now
```

After mitigation, 'uname -a' should report a kernel equal to (or newer than):

```
Linux [HOST] 3.10.0-327.36.1.el7.x86_64 #1 SMP Sun Sep 18 13:04:29 UTC 2016
x86_64 x86_64 x86_64 GNU/Linux
```

©Copyright 2015 Hewlett-Packard Enterprise Development Company, L.P.

Hewlett-Packard Enterprise Company shall not be liable for technical or editorial errors or omissions contained herein. The information provided is provided "as is" without warranty of any kind. To the extent permitted by law, neither HPE or its affiliates, subcontractors or suppliers will be liable for incidental, special or consequential damages including downtime cost; lost profits; damages relating to the procurement of substitute products or services; or damages for loss of data, or software restoration. The information in this document is subject to change without notice. Hewlett-Packard Company and the names of Hewlett-Packard Enterprise products referenced herein are trademarks of Hewlett-Packard Enterprise Company in the United States and other countries. Other product and company names mentioned herein may be trademarks of their respective owners.