

HPE Software Security Update

HPE Virtualization Performance Viewer

CVE-2015-7872

Document management:

Date	Version	Change
08/02/2016	1	Initial release

Summary:

The following article enlists the necessary related for the HPE Software Product Virtualization Performance Viewer Virtual Appliance on the CVE-2015-7872.

Topic

CVE-2015-7872 security vulnerability

<https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-7872>

Note: This link provides further information about this issue and lists the products affected.

HPE has investigated the CVE-2015-7872 security vulnerability in relation to HPE Virtualization Performance Viewer Virtual Appliance. This document provides required actions that must be performed to mitigate this vulnerability.

Affected Releases:

Product name	Affected Supported Versions
HPE Virtualization Performance Viewer	v1.20, v2.0, v2.01, v2.10, v2.20

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

Response

Impact on Virtualization Performance Viewer Virtual Appliance

HPE Virtualization Performance Viewer product was found to be vulnerable to the CVE-2015-7872. Affected versions are mentioned above in the table.

The `key_gc_unused_keys` function in `security/keys/gc.c` in the Linux kernel through 4.2.6 allows local users to cause a denial of service (OOPS) via crafted `keyctl` commands. Following are the rpms updated in HPE Cloud Optimizer (new name of vPV) 3.00 Virtual Appliance.

```
rpm name="kernel" epoch="(none)" version="2.6.32" release="573.12.1.el6" arch="x86_64"  
rpm name="kernel-firmware" epoch="(none)" version="2.6.32" release="573.12.1.el6" arch="noarch"  
rpm name="kernel-headers" epoch="(none)" version="2.6.32" release="573.12.1.el6" arch="x86_64"
```

Mitigation Actions

HP recommends that customers update to HPE Cloud Optimizer (new name of vPV) 3.00 Virtual Appliance.

Note: HPE Cloud Optimizer is new name of HPE Virtualization Performance Viewer

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

Hewlett-Packard 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 HP 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 products referenced herein are trademarks of Hewlett-Packard Company in the United States and other countries. Other product and company names mentioned herein may be trademarks of their respective owners.