Hewlett Packard Enterprise

HPE Knowledge Article

HPE Helion OpenStack - HPE Helion OpenStack 4.0.6 Release Notes

Article Number mmr_sf-EN_US000021523

Environment

- HPE Helion OpenStack 4.0.6

Issue

Users are looking for the release notes

Cause

New release of HPE Helion OpenStack 4.0.6

Resolution

The items references below are resolved in this HPE Helion OpenStack 4.0.6 release:

HPE Helion OpenStack® CVE: XML-RPC server in monasca supervisor - https://nvd.nist.gov/vuln/detail/CVE-2017-11610

HPE Linux Changes:
HPE Helion OpenStack 4.0.6 includes a new version of the hLinux operating system which has fixes for hardening opportunities and CVEs known to us and deemed to be issues not mitigated by architecture at the time of ISO creation.

Keystone user home directory hardened: Requirement that keystone user home directory be world-readable is deprecated

Additional CVEs addressed in 4.0.6:
Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Partition). - https://nvd.nist.gov/vuln/detail/CVE-2018-2562
Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). - https://nvd.nist.gov/vuln/detail/CVE-2018-2622
Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). - https://nvd.nist.gov/vuln/detail/CVE-2018-2640
Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). - https://nvd.nist.gov/vuln/detail/CVE-2018-2665
Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). - https://nvd.nist.gov/vuln/detail/CVE-2018-2668
Memory leak in the virtio_gpu_object_create function - https://nvd.nist.gov/vuln/detail/CVE-2017-10810 ##
The mq_notify function in the Linux kernel - https://nvd.nist.gov/vuln/detail/CVE-2017-11176
The http.c:skip_short_body() function - https://nvd.nist.gov/vuln/detail/CVE-2017-13089
The retr.c:fd_read_body() function - https://nvd.nist.gov/vuln/detail/CVE-2017-13090
Heap-based buffer overflow in dnsmasq before 2.78 allows remote attackers to cause a denial of service (crash) or execute arbitrary

code via a crafted DNS response. - https://nvd.nist.gov/vuln/detail/CVE-2017-14491
Heap-based buffer overflow in dnsmasq before 2.78 - https://nvd.nist.gov/vuln/detail/CVE-2017-14492
Stack-based buffer overflow in dnsmasq before 2.78 - https://nvd.nist.gov/vuln/detail/CVE-2017-14493
The mod_headers module in the Apache HTTP Server 2.2.22 - https://nvd.nist.gov/vuln/detail/CVE-2013-5704
TFTP transfer and curl/libcurl - https://nvd.nist.gov/vuln/detail/CVE-2017-1000100
curl supports "globbing" of URLs - https://nvd.nist.gov/vuln/detail/CVE-2017-1000101
All versions of the SDP server in BlueZ 5.46 and earlier are vulnerable - https://nvd.nist.gov/vuln/detail/CVE-2017-1000250
libcurl may read outside of a heap allocated buffer - https://nvd.nist.gov/vuln/detail/CVE-2017-1000254
The Linux Kernel imposes a size restriction - https://nvd.nist.gov/vuln/detail/CVE-2017-1000365
Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). -
https://nvd.nist.gov/vuln/detail/CVE-2017-10378
Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client programs). -
https://nvd.nist.gov/vuln/detail/CVE-2017-10379
Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). -
https://nvd.nist.gov/vuln/detail/CVE-2017-10384
qemu-nbd in QEMU (aka Quick Emulator) does not ignore SIGPIPE - https://nvd.nist.gov/vuln/detail/CVE-2017-10664
The make_response function in drivers/block/xen-blkback/blkback.c - https://nvd.nist.gov/vuln/detail/CVE-2017-10911
dnsmasq before 2.78 - https://nvd.nist.gov/vuln/detail/CVE-2017-14494
Memory leak in dnsmasq before 2.78 - https://nvd.nist.gov/vuln/detail/CVE-2017-14495
Integer underflow in the add_pseudoheader function in dnsmasq before 2.78 - https://nvd.nist.gov/vuln/detail/CVE-2017-14496
IPAddressFamily extension in an X.509 certificate - https://nvd.nist.gov/vuln/detail/CVE-2017-3735
vmw_gb_surface_define_ioctl function - https://nvd.nist.gov/vuln/detail/CVE-2017-7346
Race condition in the fsnotify implementation - https://nvd.nist.gov/vuln/detail/CVE-2017-7533
The brcmf_cfg80211_mgmt_tx function - https://nvd.nist.gov/vuln/detail/CVE-2017-7541
The ip6_find_1stfragopt function - https://nvd.nist.gov/vuln/detail/CVE-2017-7542
The vmw_gb_surface_define_ioctl function - https://nvd.nist.gov/vuln/detail/CVE-2017-9605
The SSL protocol - https://nvd.nist.gov/vuln/detail/CVE-2011-3389
Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication) -
https://nvd.nist.gov/vuln/detail/CVE-2017-10268
x86_64 Montgomery squaring procedure in OpenSSL - https://nvd.nist.gov/vuln/detail/CVE-2017-3736
Keberos 5 tickets being decoded when using the RXRPC keys incorrectly assumes the size of a field. -
https://access.redhat.com/security/cve/cve-2017-7482
A use-after-free flaw was found in the TLS 1.2 implementation - https://access.redhat.com/security/cve/cve-2017-7805
QEMU (aka Quick Emulator), when built with the e1000e NIC emulation support - https://nvd.nist.gov/vuln/detail/CVE-2017-9310
QEMU (aka Quick Emulator) before 2.9.0, when built with the USB OHCI Emulation support -
https://nvd.nist.gov/vuln/detail/CVE-2017-9330
Memory leak in QEMU (aka Quick Emulator) - https://nvd.nist.gov/vuln/detail/CVE-2017-9373
Memory leak in QEMU (aka Quick Emulator), when built with USB EHCI Emulation support -
https://nvd.nist.gov/vuln/detail/CVE-2017-9374
QEMU (aka Quick Emulator), when built with USB xHCI controller emulator support - https://nvd.nist.gov/vuln/detail/CVE-2017-9375
Git uses unsafe Perl scripts - https://nvd.nist.gov/vuln/detail/CVE-2017-14867

For more information on security vulnerabilities, please see the National Vulnerability Database: https://nvd.nist.gov/

Known issues in this release:
Adding RHEL compute support during upgrade:
If a cloud was deployed without RHEL compute support but it is being added during the upgrade a disruption may occur with some OpenStack
services. This only happens if the RHEL profile does not already exist in cobbler but a RHEL ISO has been placed in the home directory. This
can be resolved by the following workaround procedure:
log in to the deployer node
as root, create folder /mnt/rhel7_iso
cd /home/stacks/scratch/ansible/next/hos/ansible/
edit the roles/cobbler/tasks/populate-rhel.ymp playbook and change all 3 instances of /mnt to /mnt/rhel7_iso
line 57: mount -o loop "{{hlmuser_home}}/{{deployer_rhel7_iso}}" "/mnt/rhel7_iso"
line 64: --path /mnt/rhel7_iso

line 84: umount /mnt/rhel7_iso
edit the roles/cobbler/tasks/get-rhel-loader.yml playbook and change all 4 instances of /mnt to /mnt/rhel7_iso
line 26: name: /mnt/rhel7_iso
line 46: - /mnt/rhel7_iso
line 47: - /mnt/rhel7_iso
line 52: name: /mnt/rhel7_iso
run the upgrade as described.

Warning: If your system is currently on version HPE Helion OpenStack 4.0.6 the correct upgrade path is to HPE Helion OpenStack 5.0.3

The full extract of the HPE Helion OpenStack 4.0 release notes for all 4.x releases is available on our FTP site as referenced on www.hpe.com/Helion/docs