Twin Cities
Red Hat Users Group
Q1/2016

Agenda

- **Introductions / Announcements** by Marc Skinner from Red Hat
- **SAP Clustering** by Sherry Yu from Red Hat
- **Ansible 2.0** by David Federlein from Ansible / Red Hat
- **OpenStack Liberty** by Ian Pilcher from Red Hat
- **DM-Cache** by Marc Skinner from Red Hat
- **RHEL in Azure** by Marc Skinner from Red Hat

Announcements

- Upcoming – *dates subject to change ***
    - RHEL 6.8 is targeting late Q2 2016
    - RHEL 7.3 is targeting Q4 2016
    - OSP8 (Liberty) is targeting any day
    - OSE 3.2 is targeting late Q2 2016
    - RHEV 3.6 targeting late Q1 2016
    - Satellite 6.2 is targeting early Q3 2016

- Reminder
    - Red Hat Summit :: June 28-July 1st, 2016 in San Francisco
    - Satellite 5.5 and earlier EOL May 29, 2015
    - Satellite 5.6 and 5.7 supported until March 31, 2017

Minneapolis Storage Day Event

- April 12 :: 1-6pm
- Agenda
  - Why Software Defined Storage Matters
  - Customer Spotilight – Target
  - Ceph on Intel
  - Ceph Performance Update
  - Red Hat Storage for Containerized Applications
  - Red Hat Storage Roadmap

Special Guests

- Jessica Sawyer, Sherry Yu and Ted Jones – Red Hat SAP team/relationship

Proactive Notifications

LOCAL : sos security and bug fix update

(CVE-2015-7529)

The sos package contains a set of tools that gather information from system hardware, logs and configuration files. The information can then be used for diagnostic purposes and debugging.

An insecure temporary file use flaw was found in the way sos created certain sosreport files. A local attacker could possibly use this flaw to perform a symbolic link attack to reveal the contents of sosreport files, or in some cases modify arbitrary files and escalate their privileges on the system. (CVE-2015-7529)

https://rhn.redhat.com/errata/RHSA-2016-0152.html
https://access.redhat.com/security/cve/cve-2015-7529

Proactive Notifications

LOCAL : use-after-free vulnerability in kernel keyring facility

(CVE-2016-0728)

A use-after-free flaw was found in kernel keyring facility, possibly leading to local privilege escalation, the keyring facility is primarily a way for drivers to retain or cache security data, authentication keys, encryption keys and other data in the kernel.

https://access.redhat.com/articles/2131021
https://access.redhat.com/security/cve/cve-2016-0728

Proactive Notifications

OpenSSH: Information-leak vulnerability

(CVE-2016-0777)

An information leak flaw was found in the way OpenSSH client roaming feature was implemented. The information leak is exploitable in the default configuration of certain versions of the OpenSSH client and could (depending on the client's version, compiler, and operating system) allow a malicious SSH server to steal the client's private keys.

https://access.redhat.com/articles/2123781
https://access.redhat.com/security/cve/CVE-2016-0777

Proactive Notifications

Critical security flaw: glibc stack-based buffer overflow in getaddrinfo()

(CVE-2015-7547)

A stack-based buffer overflow was found in the way the libresolv library performed dual A/AAAA DNS queries. A remote attacker could create a specially crafted DNS response which could cause libresolv to crash or, potentially, execute code with the permissions of the user running the library. Note: this issue is only exposed when libresolv is called from the nss_dns NSS service module.

https://access.redhat.com/security/cve/cve-2015-7547
https://bugzilla.redhat.com/show_bug.cgi?id=1293532