A PROBLEM’S NOT A PROBLEM, UNTIL IT’S A PROBLEM.

Red Hat Insights

Phil Griffiths
Senior Solutions Architect
May 2018
WHY IS INSIGHTS SO GOOD?
SaaS  2 mins

PERFORMANCE
AVAILABILITY
STABILITY
SECURITY
GETTING STARTED
[root@server ~]# subscription-manager register --auto-attach
[root@server ~]# yum install redhat-access-insights
[root@server ~]# redhat-access-insights --register

https://access.redhat.com/insights/overview/
USE CASES
OPERATIONS / DEVOPS / SRE
**Critical Risk Actions**

Actions identified with a critical level of risk

<table>
<thead>
<tr>
<th>Rule</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Total Risk</th>
<th>Systems</th>
<th>Ansible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dnsmasq with listening processes vulnerable to remote code execution via crafted DNS requests (CVE-2017-14491)</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
<td>4</td>
<td>🟢</td>
</tr>
</tbody>
</table>

Show rules without actions (6 more)
Dnsmasq with listening processes vulnerable to remote code execution via crafted DNS requests (CVE-2017-14491)

A vulnerability was discovered in Dnsmasq which allows an attacker to overflow a heap buffer and crash or take control of Dnsmasq. This is accomplished through DNS requests to Dnsmasq querying a domain controlled by the attacker.

Dnsmasq is a popular lightweight DNS and DHCP server, often used in home networks and cloud environments as a caching DNS stub resolver and to manage DHCP leases. It is used either standalone or directly by applications including libviri, and in a number of layered products. Libvirt is a management tool for managing Linux containers and virtual machines.

This vulnerability can lead to remote code execution and could be triggered by a malicious user on the network.

Red Hat recommends that you update Dnsmasq packages to include the CVE-2017-14491 security release.

4 Impacted Systems

- RHEL Server isinode1.ose3.peterlarsen.org (9 hours ago)
- RHEL Server isinode2.ose3.peterlarsen.org (8 hours ago)
- RHEL Server isinode3.ose3.peterlarsen.org (12 hours ago)
- RHEL Server isinode4.ose3.peterlarsen.org (8 hours ago)
SYSTEM ADMINISTRATORS
Your weekly Insights report

Hi Phil,

You currently have 66 systems registered with Insights and 11 high severity hits.

There have been 4 new rules added to Insights since your last weekly report:

- **Nova commands timeout when the growing versioned notifications queues have no consumers**
  Nova commands timeout because growing versioned notifications queues have no consumers.

- **Pod creation fails when is under high load due to iptables-restore process**
  Pod creation fails when is under high load due to iptables-restore process.

- **Network performance degradation when PMD cores are not present in isolcpus list**
  All PMD Driver (PMD) masked CPU cores should be isolated from the host OS so that the CPU cores will not be used by the host OS. Otherwise Data Plane Development Kit (DPDK) network performance will be degraded.

- **NetworkManager fails to set default gateway for teaming VLAN devices at boot time due to a known bug**
  At boot time, NetworkManager fails to set default gateway on LACP interfaces (bonding/teaming) configured as VLAN interfaces, which can cause connectivity loss due to a known bug in NetworkManager.

We want you to get the most out of Insights and would love to hear your questions and comments. Feel free to email us at insights+weekly@redhat.com, and we'll get back to you as soon as we can.
SECURITY PROFESSIONALS
The line graph shows a peak in Score on March 19, followed by a decline and fluctuation over the period from March 10 to April 6, 2018. The Score values range from around 685 to 750 during this period.
<table>
<thead>
<tr>
<th>Rule</th>
<th>Impacted Systems</th>
<th>Total Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dnsmasq with listening processes vulnerable to remote code execution via crafted DNS requests (CVE-2017-14491)</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>Startup failure for AWT java applications when invalid fonts are installed</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>IPA server upgrade failed when IPv6 is disabled</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>memcached UDP server allows spoofed traffic amplification DoS (CVE-2018-1000115)</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Dnsmasq vulnerable to remote code execution via crafted DNS requests (CVE-2017-14491)</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>wpa_supplicant is vulnerable to man-in-the-middle attack via crafted WPA2 frames (CVE-2017-13077)</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Kernel vulnerable to side-channel attacks in modern microprocessors (CVE-2017-5753/Spectre, CVE-2017-5754/Meltdown)</td>
<td>61</td>
<td></td>
</tr>
</tbody>
</table>
SUMMARY
ZERO INFRASTRUCTURE
QUICK TO GET STARTED
IMMEDIATELY EFFECTIVE
AUTOMATED REMEDIATION
THANK YOU

plus.google.com/+RedHat
linkedin.com/company/red-hat
youtube.com/user/RedHatVideos
facebook.com/redhatinc
twitter.com/RedHatNews