



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?

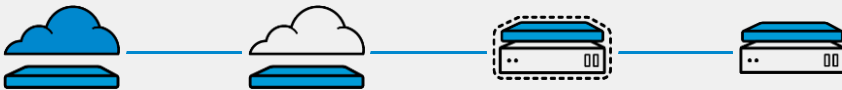
SaaS 2 mins



PERFORMANCE
AVAILABILITY
STABILITY
SECURITY



ANSIBLE



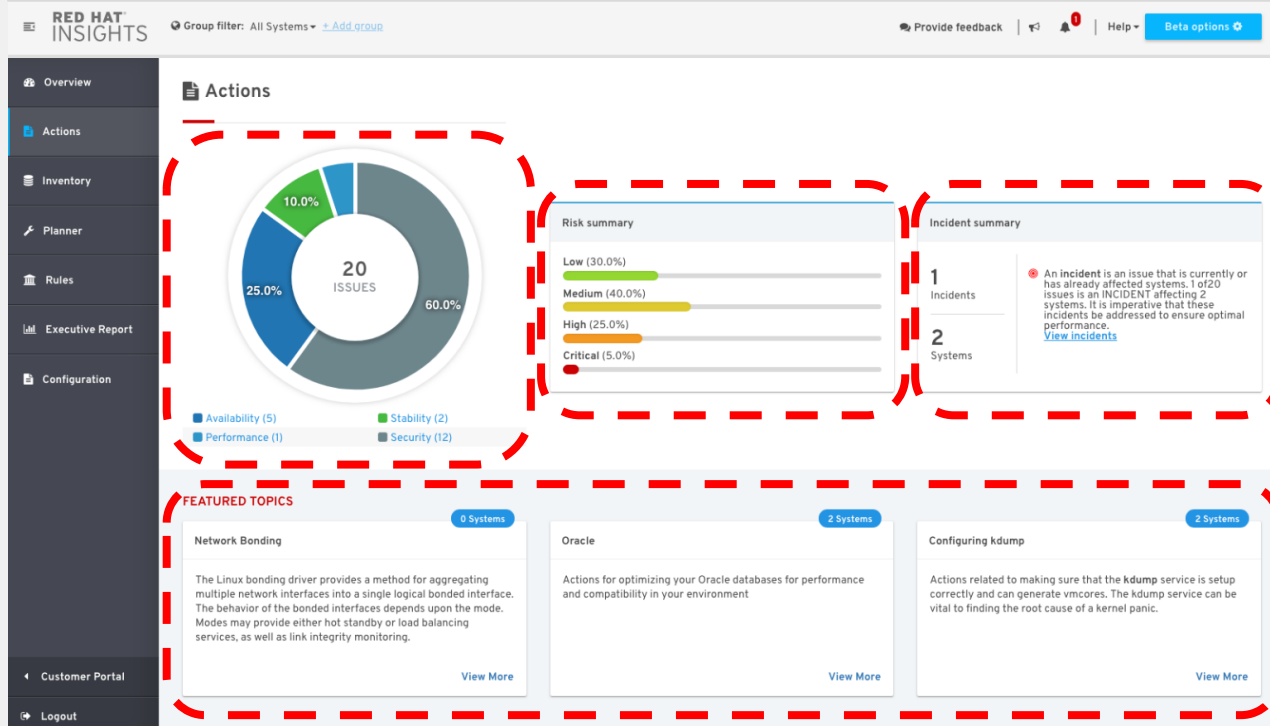
GETTING STARTED

1

2

```
[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





GULP!


 **RED HAT**
INSIGHTS


Group filter: All Systems ▾ [+ Add group](#)


Provide feedback |   | Help ▾ [Try Insights Beta](#)


 Overview


 Actions

 Inventory

 Planner

 Rules


 Executive Report

 Configuration

Actions / Critical Risk Actions

Critical Risk Actions

Actions identified with a critical level of risk





Search rules 

Total Risk

All ▾

Risk of Change

All ▾

Rule	Likelihood	Impact	Total Risk	Systems	Ansible
Dnsmasq with listening processes vulnerable to remote code execution via crafted DNS requests (CVE-2017-14491)				4	

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 libvirt, 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.



Impact

Likelihood

Total Risk

 Risk of change: **Very Low**

Find a system



Check in status

All

Actions ▾

4 Impacted Systems



Type



Name



RHEL Server

[isonode1.ose3.peterlarsen.org](#)

RHEL Server

[isonode2.peterlarsen.org](#)

RHEL Server

[isonode3.ose3.peterlarsen.org](#)

RHEL Server

[isonode4.ose3.peterlarsen.org](#)

Reported

9 hours ago

8 hours ago

12 hours ago

8 hours ago



SYSTEM ADMINISTRATORS



CONTROL 1

CONFIGURE 2

RESTRICT 3

EXTEND 4



RED HAT® INSIGHTS

Weekly Report for April 9, 2018

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 Pull Mode 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



[Overview](#)[Actions](#)[Inventory](#)[Planner](#)[Rules](#)[Executive Report](#)[Configuration](#)[Customer Portal](#)[Logout](#)

Overall score



Weekly action count by category

10

SECURITY

5

AVAILABILITY

1

STABILITY

0

PERFORMANCE

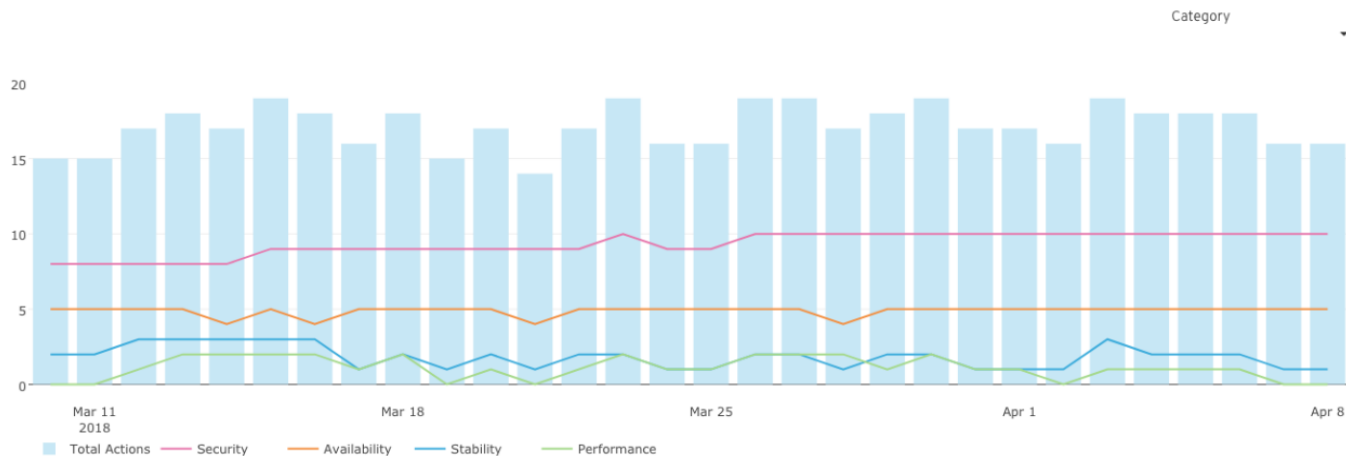
✓ You've resolved 17 issues in the past 30 days.

ACTION TRENDS

ACTIVE SYSTEMS

SCORE HISTORY

ALL RULE HITS

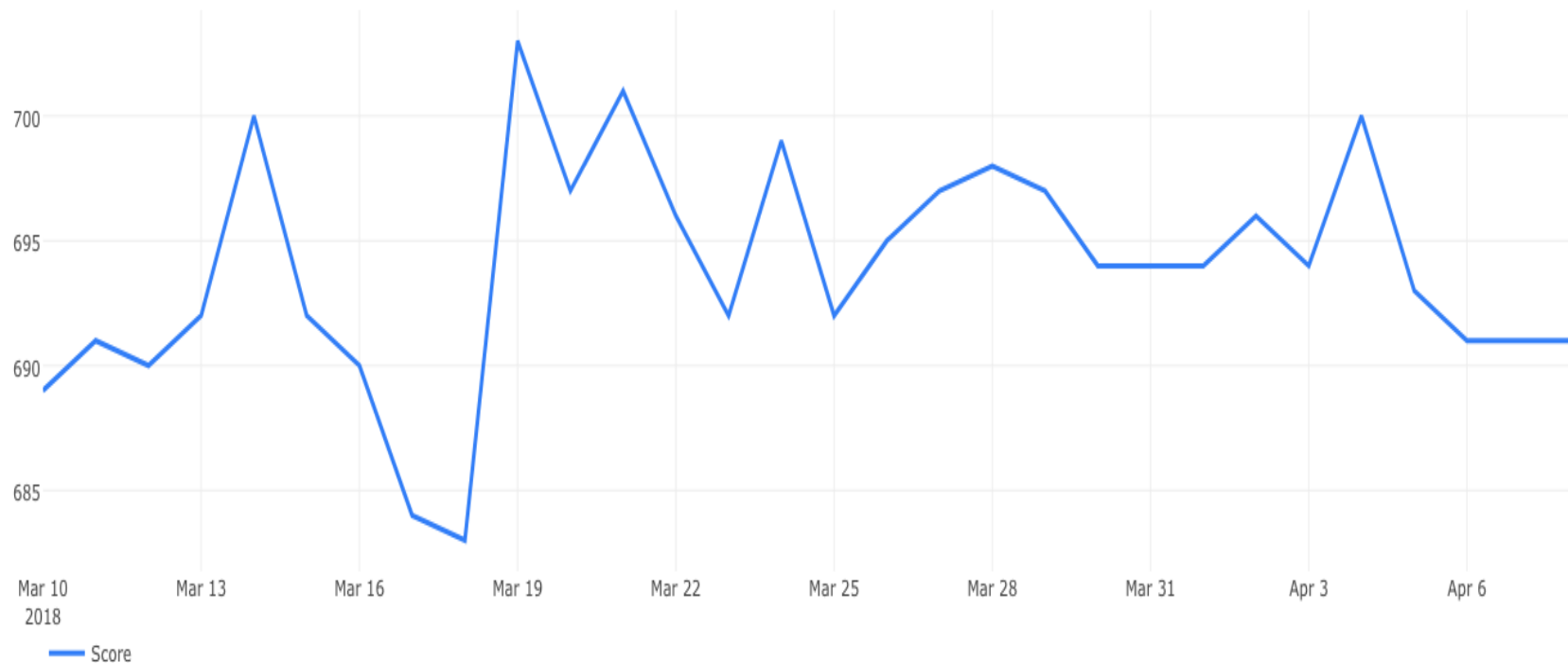


ACTION TRENDS

ACTIVE SYSTEMS

SCORE HISTORY

ALL RULE HITS



[ACTION TRENDS](#)[ACTIVE SYSTEMS](#)[SCORE HISTORY](#)[ALL RULE HITS](#)

Rule	Impacted Systems	Total Risk
Dnsmasq with listening processes vulnerable to remote code execution via crafted DNS requests (CVE-2017-14491)	4	
Startup failure for AWT java applications when invalid fonts are installed	6	
IPA server upgrade failed when IPv6 is disabled	2	
memcached UDP server allows spoofed traffic amplification DoS (CVE-2018-1000115)	1	
Dnsmasq vulnerable to remote code execution via crafted DNS requests (CVE-2017-14491)	1	
wpa_supplicant is vulnerable to man-in-the-middle attack via crafted WPA2 frames (CVE-2017-13077)	1	
Kernel vulnerable to side-channel attacks in modern microprocessors (CVE-2017-5753/Spectre, CVE-2017-5754/Meltdown)	61	

SUMMARY

ZERO INFRASTRUCTURE

QUICK TO GET STARTED

IMMEDIATELY EFFECTIVE

AUTOMATED REMEDIATION



RED HAT
SUMMIT

THANK YOU



plus.google.com/+RedHat



facebook.com/redhatinc



linkedin.com/company/red-hat



twitter.com/RedHatNews



youtube.com/user/RedHatVideos