Vulnerabilities report

ID	Name	IP	Version	Manager	OS
029	S-DEMO-SIT01	10.101.4.38	Wazuh v3.9.5	S-DEMO-SEC01.example.com	CentOS Linux 7.6

Registration date: 2019-09-11 08:04:04.

Last keep alive: 2019-09-11 10:12:15.

Group: default

Discover what applications in your environment are affected by well-known vulnerabilities.

🕘 2019-09-11T16:12:01 to 2019-09-11T18:12:01

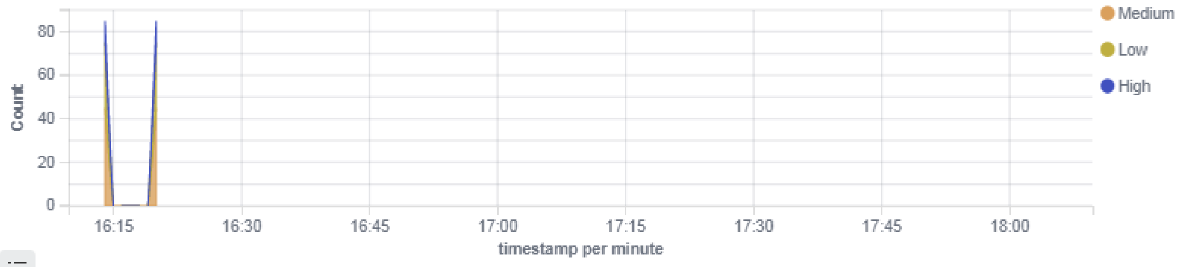
🔍 manager.name: S-DEMO-SEC01.example.com AND rule.groups: vulnerability-detector AND agent.id: 029

High severity

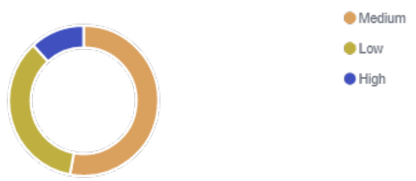
Click on each link to read more about each found vulnerability.

- kernel
  - https://access.redhat.com/security/cve/CVE-2018-12130
  - https://access.redhat.com/security/cve/CVE-2019-11085
  - https://access.redhat.com/security/cve/CVE-2019-11477
  - https://access.redhat.com/security/cve/CVE-2019-13272
  - https://access.redhat.com/security/cve/CVE-2019-3900
  - https://access.redhat.com/security/cve/CVE-2019-5489
  - https://access.redhat.com/security/cve/CVE-2019-9213
  - https://access.redhat.com/security/cve/CVE-2019-9500
- python-jinja2
  - https://access.redhat.com/security/cve/CVE-2019-10906
- wget
  - https://access.redhat.com/security/cve/CVE-2019-5953

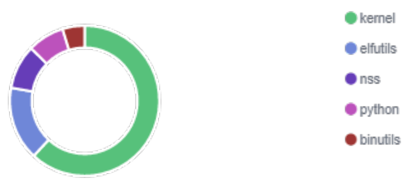
Alerts severity over time



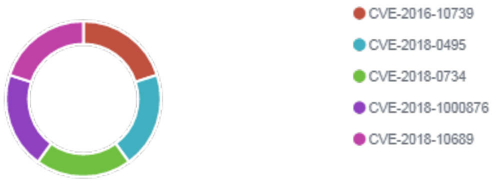
Severity distribution



Top 5 affected packages



Most common CVEs



Most common rules

Rule ID	Description	Count
23503	Kernel: KVM: leak of uninitialized stack contents to guest	2
23504	Kernel: tcp: excessive resource consumption while processing SACK blocks allows remote denial of service	2
23505	Kernel: page cache side channel attacks	2

Alerts summary

Severity	Title	Reference	CVE	Count
High	Kernel: page cache side channel attacks	https://access.redhat.com/security/cve/CVE-2019-5489	CVE-2019-5489	2
High	Kernel: tcp: integer overflow while processing SACK blocks allows remote denial of service	https://access.redhat.com/security/cve/CVE-2019-11477	CVE-2019-11477	2
High	Kernel: vhost_net: infinite loop while receiving packets leads to DoS	https://access.redhat.com/security/cve/CVE-2019-3900	CVE-2019-3900	2
High	hardware: Microarchitectural Fill Buffer Data Sampling (MFBDS)	https://access.redhat.com/security/cve/CVE-2018-12130	CVE-2018-12130	2
High	kernel: brcmfmac heap buffer overflow in brcmf_wowl_nd_results	https://access.redhat.com/security/cve/CVE-2019-9500	CVE-2019-9500	2
Low	Kernel: KVM: leak of uninitialized stack contents to guest	https://access.redhat.com/security/cve/CVE-2019-7222	CVE-2019-7222	2
Low	binutils: NULL pointer dereference in work_stuff_copy_to_from in cplus-dem.c.	https://access.redhat.com/security/cve/CVE-2018-12697	CVE-2018-12697	2
Low	binutils: Stack Exhaustion in the demangling functions provided by libiberty	https://access.redhat.com/security/cve/CVE-2018-12641	CVE-2018-12641	2
Low	blktrace: buffer overflow in the dev_map_read function in btt/devmap.c	https://access.redhat.com/security/cve/CVE-2018-10689	CVE-2018-10689	2
Low	curl: Heap-based buffer over-read in the curl tool warning formatting	https://access.redhat.com/security/cve/CVE-2018-16842	CVE-2018-16842	2
Medium	Kernel: tcp: excessive resource consumption while processing SACK blocks allows remote denial of service	https://access.redhat.com/security/cve/CVE-2019-11478	CVE-2019-11478	2
Medium	ROHNP: Key Extraction Side Channel in Multiple Crypto Libraries	https://access.redhat.com/security/cve/CVE-2018-0495	CVE-2018-0495	2
Medium	binutils: integer overflow leads to heap-based buffer overflow in objdump	https://access.redhat.com/security/cve/CVE-2018-1000876	CVE-2018-1000876	2
Medium	glibc: getaddrinfo should reject IP addresses with trailing characters	https://access.redhat.com/security/cve/CVE-2016-10739	CVE-2016-10739	2
Medium	hardware: Micro-architectural Load Port Data Sampling - Information Leak (MLPDS)	https://access.redhat.com/security/cve/CVE-2018-12127	CVE-2018-12127	2