Vulnerabilities report

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

2020-10-06T03:56:20 to 2020-10-06T09:56:20

manager.name: dhsiem.verse.in AND rule.groups: vulnerability-detector AND agent.name : "RENT-ARP-LT5126"

Summary

- 1 of 41 agents have high vulnerabilities.
- 1 of 41 agents have medium vulnerabilities.

Top 3 agents with high severity vulnerabilities

ID	Name	IP	Version	Manager	OS	Registration date	Last keep alive
012	RENT-ARP-LT5126	169.254.227.161	Wazuh v3.13.1	dhsiem.verse.in	Microsoft Windows 10 Pro 10.0.19041	2020-09-02 12:29:53	2020-10-06 04:24:49

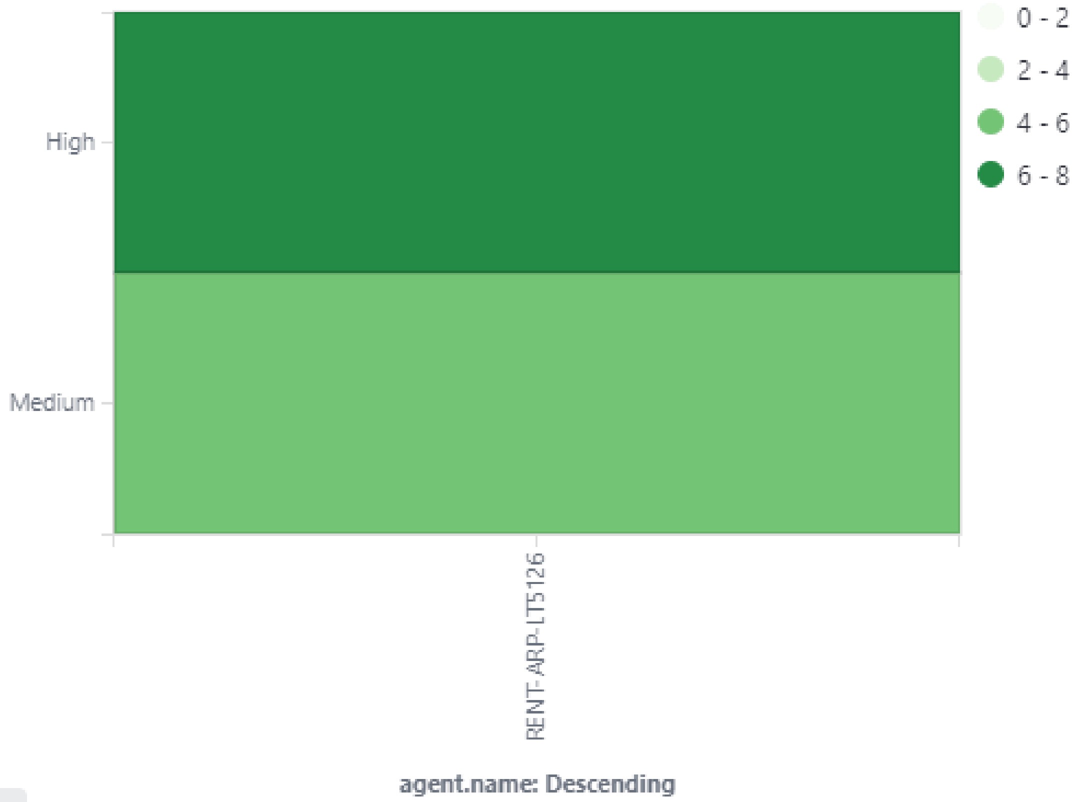
Top 3 agents with medium severity vulnerabilities

ID	Name	IP	Version	Manager	OS	Registration date	Last keep alive
012	RENT-ARP-LT5126	169.254.227.161	Wazuh v3.13.1	dhsiem.verse.in	Microsoft Windows 10 Pro 10.0.19041	2020-09-02 12:29:53	2020-10-06 04:24:49

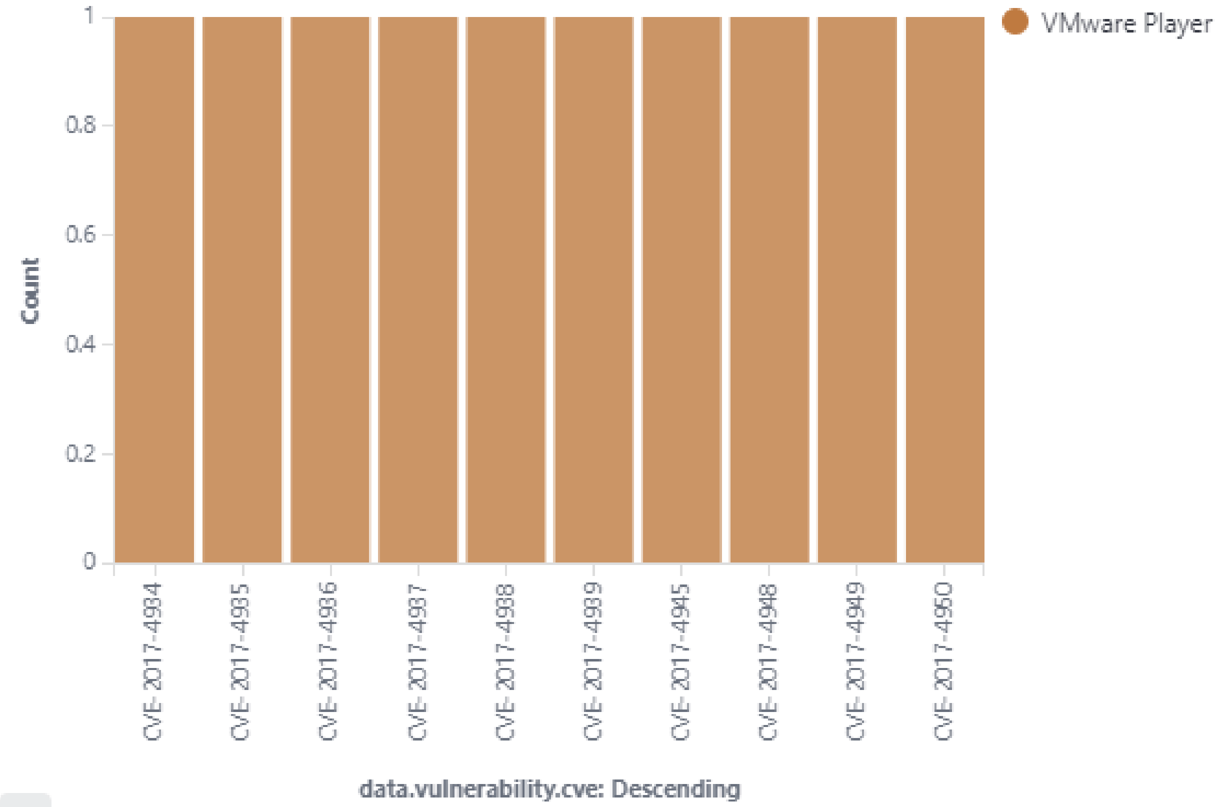
Top 3 CVE

Top	CVE
1	CVE-2017-4934
2	CVE-2017-4935
3	CVE-2017-4936

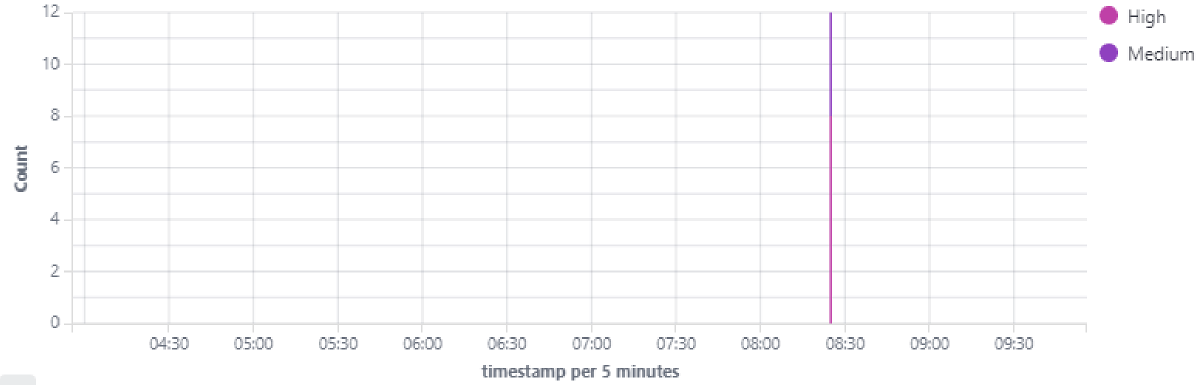
Agents by severity



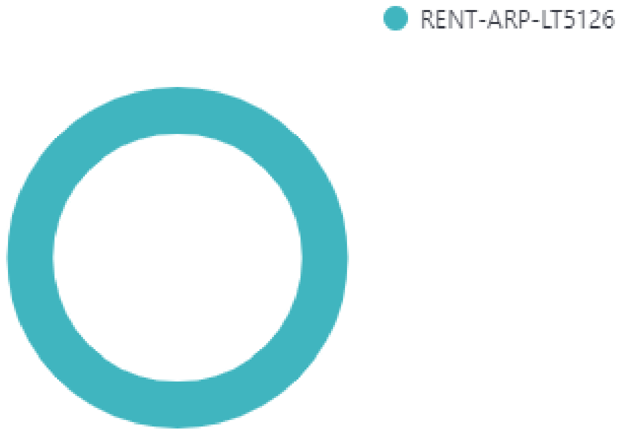
Top affected packages by CVEs



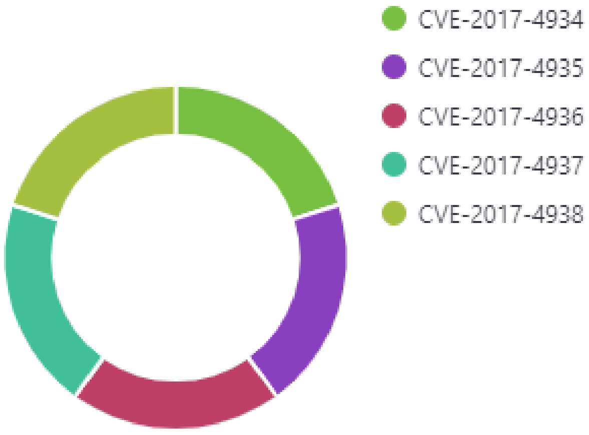
Severity count



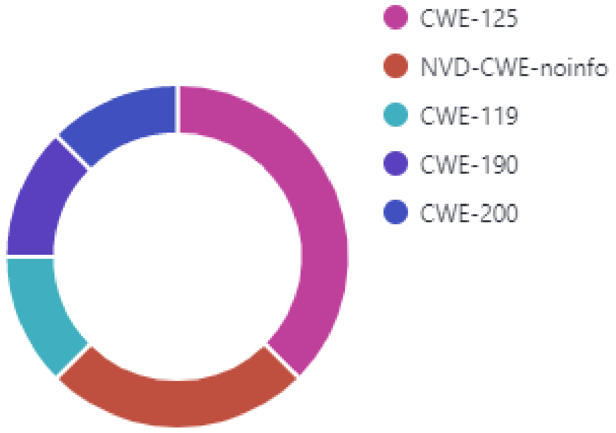
Most affected agents



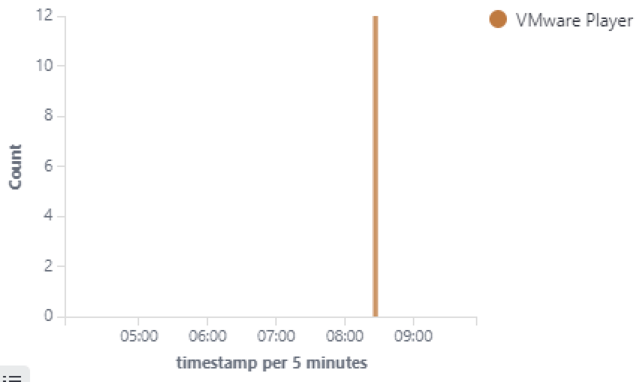
Most common CVEs



Most common CWEs



TOP affected packages alerts Evolution



Alert summary

Severity	Title	Published	CVE	Count
High	VMware Workstation (12.x before 12.5.8) and Fusion (8.x before 8.5.9) contain a heap buffer-overflow vulnerability in VMNAT device. This issue may allow a guest to execute code on the host.	1510876800000	CVE-2017-4934	1
High	VMware Workstation (12.x before 12.5.8) and Horizon View Client for Windows (4.x before 4.6.1) contain an out-of-bounds read vulnerability in JPEG2000 parser in the TPView.dll. On Workstation, this may allow a guest to execute code or perform a Denial of Service on the Windows OS that runs Workstation. In the case of a Horizon View Client, this may allow a View desktop to execute code or perform a Denial of Service on the Windows OS that runs the Horizon View Client.	1510876800000	CVE-2017-4936	1
High	VMware Workstation (12.x before 12.5.8) and Horizon View Client for Windows (4.x before 4.6.1) contain an out-of-bounds read vulnerability in JPEG2000 parser in the TPView.dll. On Workstation, this may allow a guest to execute code or perform a Denial of Service on the Windows OS that runs Workstation. In the case of a Horizon View Client, this may allow a View desktop to execute code or perform a Denial of Service on the Windows OS that runs the Horizon View Client. Exploitation is only possible if virtual printing has been enabled. This feature is not enabled by default on Workstation but it is enabled by default on Horizon View Client.	1510876800000	CVE-2017-4937	1
High	VMware Workstation (12.x before 12.5.8) and Horizon View Client for Windows (4.x before 4.6.1) contain an out-of-bounds write vulnerability in JPEG2000 parser in the TPView.dll. On Workstation, this may allow a guest to execute code or perform a Denial of Service on the Windows OS that runs Workstation. In the case of a Horizon View Client, this may allow a View desktop to execute code or perform a Denial of Service on the Windows OS that runs the Horizon View Client. Exploitation is only possible if virtual printing has been enabled. This feature is not enabled by default on Workstation but it is enabled by default on Horizon View Client.	1510876800000	CVE-2017-4935	1
High	VMware Workstation (12.x before 12.5.8) installer contains a DLL hijacking issue that exists due to some DLL files loaded by the application improperly. This issue may allow an attacker to load a DLL file of the attacker's choosing that could execute arbitrary code.	1510876800000	CVE-2017-4939	1
Medium	Systems with microprocessors utilizing speculative execution and branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis.	1515024000000	CVE-2017-5753	1
Medium	VMware Workstation (12.x before 12.5.8) and Fusion (8.x before 8.5.9) contain a guest RPC NULL pointer dereference vulnerability. Successful exploitation of this issue may allow attackers with normal user privileges to crash their VMs.	1510876800000	CVE-2017-4938	1
Medium	VMware Workstation (14.x and 12.x) and Fusion (10.x and 8.x) contain a guest access control vulnerability. This issue may allow program execution via Unity on locked Windows VMs. VMware Tools must be updated to 10.2.0 for each VM to resolve CVE-2017-4945. VMware Tools 10.2.0 is consumed by Workstation 14.1.0 and Fusion 10.1.0 by default.	1515110400000	CVE-2017-4945	1
Medium	VMware Workstation (14.x before 14.1.1, 12.x) and Fusion (10.x before 10.1.1 and 8.x) contain a denial-of-service vulnerability which can be triggered by opening a large number of VNC sessions. Note: In order for exploitation to be possible on Workstation and Fusion, VNC must be manually enabled.	1521072000000	CVE-2018-6957	1