info@wazuh.com
https://wazuh.com

Vulnerabilities report

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

2020-10-06T03:53:39 to 2020-10-06T09:53:39

manager.name: dhsiem.verse.in AND rule.groups: vulnerability-detector AND agent.name : "RENT-ARP-LT5111"

Summary

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

Top 3 agents with high severity vulnerabilities

ID	Name	IP	Version	Manager	OS	Registration date	Last keep alive
015	RENT-ARP-LT5111	172.16.3.2	Wazuh v3.13.1	dhsiem.verse.in	Microsoft Windows 10 Pro 10.0.18363	2020-09-02 18:05:56	2020-10-06 04:22:37

Top 3 agents with medium severity vulnerabilities

ID	Name	IP	Version	Manager	OS	Registration date	Last keep alive
015	RENT-ARP-LT5111	172.16.3.2	Wazuh v3.13.1	dhsiem.verse.in	Microsoft Windows 10 Pro 10.0.18363	2020-09-02 18:05:56	2020-10-06 04:22:37

Top 3 agents with low severity vulnerabilities

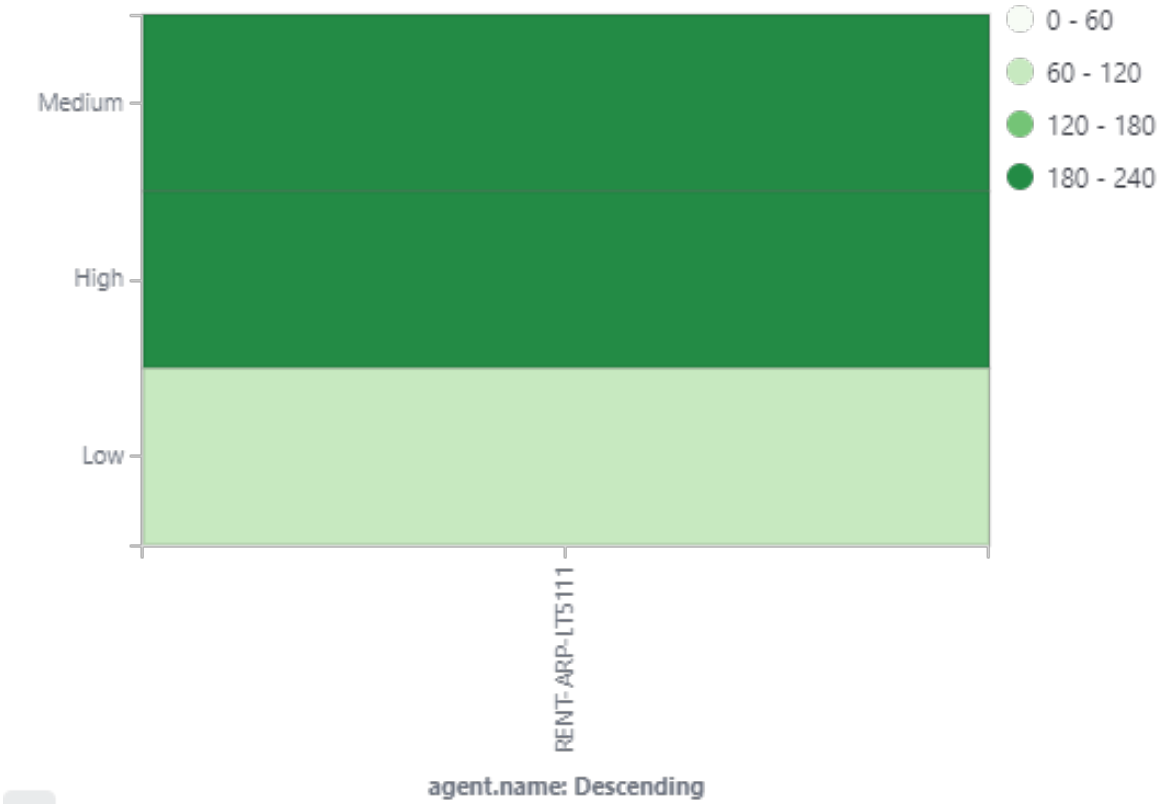
ID	Name	IP	Version	Manager	OS	Registration date	Last keep alive
015	RENT-ARP-LT5111	172.16.3.2	Wazuh v3.13.1	dhsiem.verse.in	Microsoft Windows 10 Pro 10.0.18363	2020-09-02 18:05:56	2020-10-06 04:22:37

Top 3 CVE

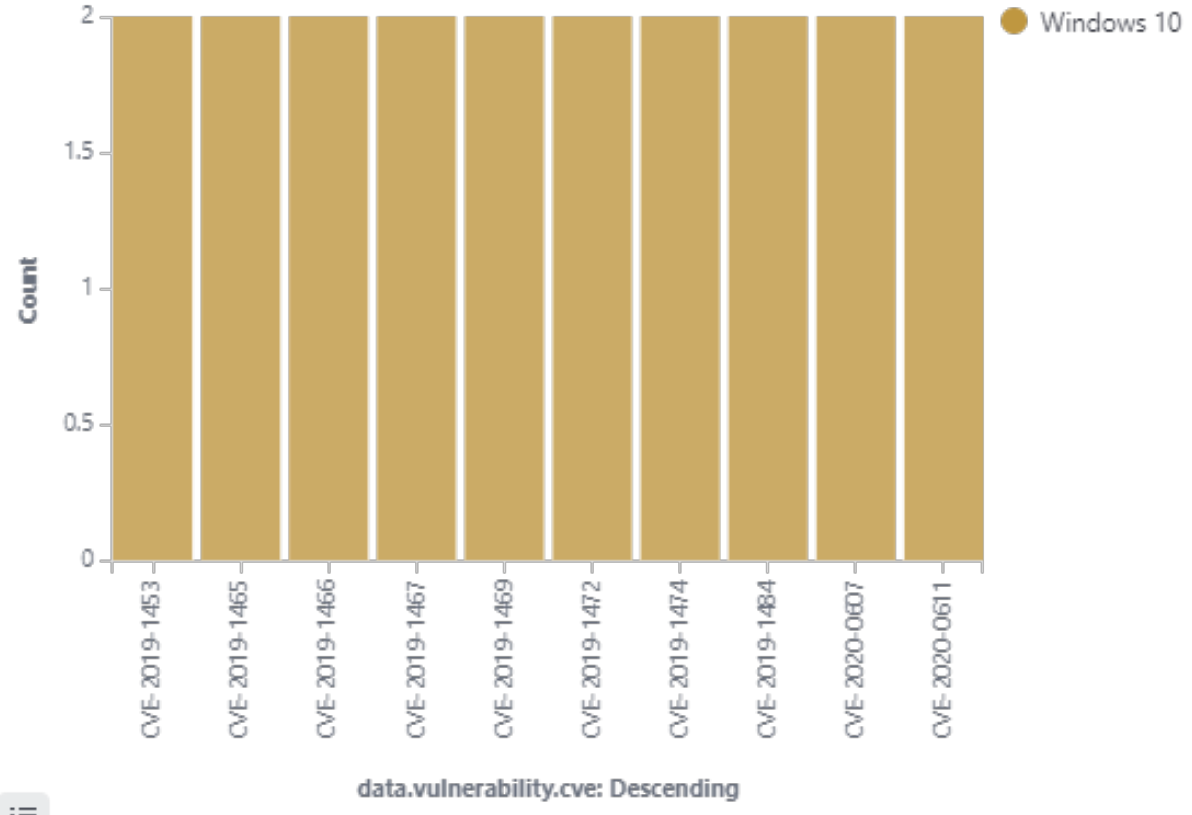
Top	CVE

Top	CVE
1	CVE-2019-1453
2	CVE-2019-1465
3	CVE-2019-1469

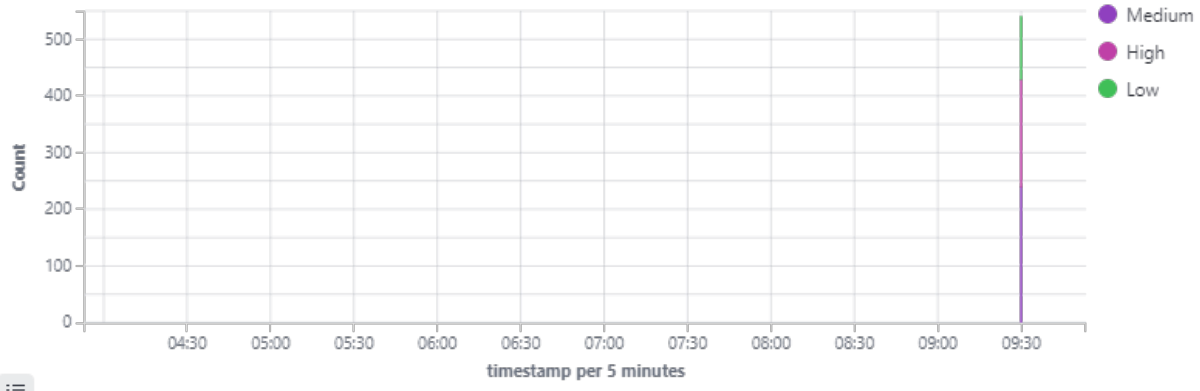
Agents by severity



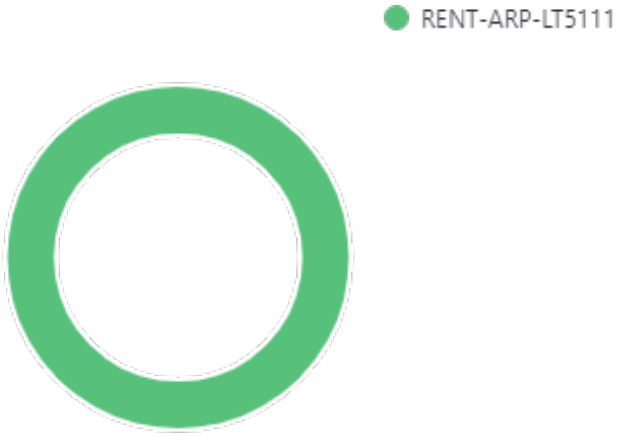
Top affected packages by CVEs



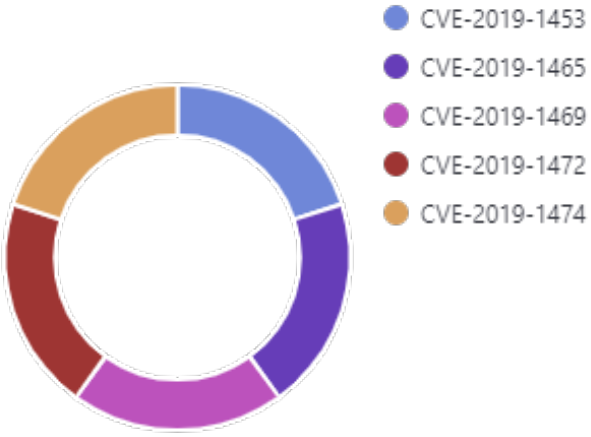
Severity count



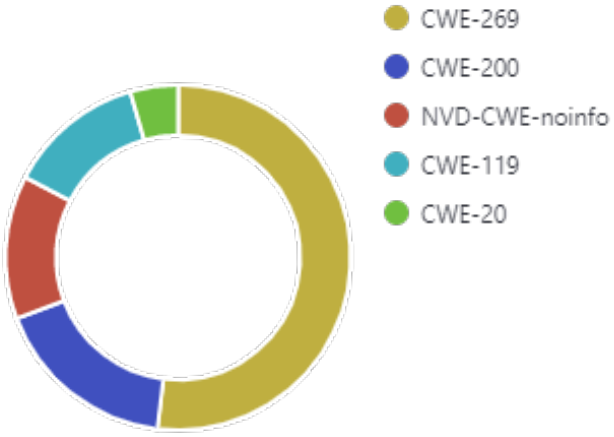
Most affected agents



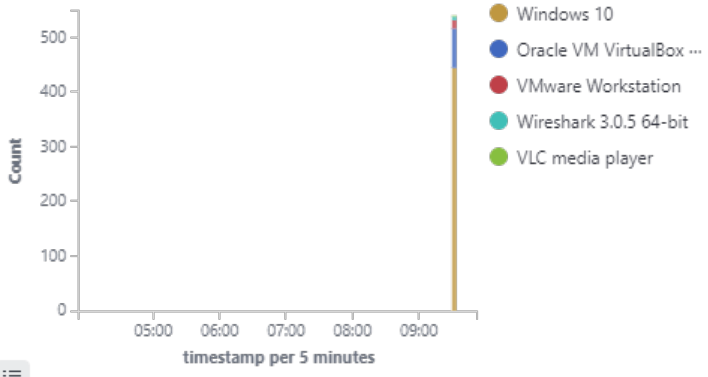
Most common CVEs



Most common CWEs



TOP affected packages alerts Evolution



Alert summary

Severity	Title	Published	CVE	Count
High	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'.	1581379200000	CVE-2020-0738	2
High	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0801, CVE-2020-0807, CVE-2020-0869.	1583971200000	CVE-2020-0809	2
High	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0948, CVE-2020-0949.	1586908800000	CVE-2020-0950	2
High	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0948, CVE-2020-0950.	1586908800000	CVE-2020-0949	2
High	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0949, CVE-2020-0950.	1586908800000	CVE-2020-0948	2
Low	An elevation of privilege vulnerability exists when the Windows User Profile Service (ProfSvc) improperly handles symlinks, aka 'Windows User Profile Service Elevation of Privilege Vulnerability'.	1581379200000	CVE-2020-0730	2
Low	An elevation of privilege vulnerability exists when the Windows User Profile Service (ProfSvc) improperly handles symlinks, aka 'Windows User Profile Service Elevation of Privilege Vulnerability'.	1583971200000	CVE-2020-0785	2
Low	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'.	1575936000000	CVE-2019-1469	2
Low	A security feature bypass vulnerability exists when Microsoft Defender improperly handles specific buffers, aka 'Microsoft Defender Security Feature Bypass Vulnerability'.	1575936000000	CVE-2019-1488	2
Low	An elevation of privilege vulnerability exists in the Windows Installer when MSI packages process symbolic links, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0798, CVE-2020-0814, CVE-2020-0842, CVE-2020-0843.	1583971200000	CVE-2020-0779	2
Medium	A denial of service vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability'.	1575936000000	CVE-2019-1453	2
Medium	A denial of service vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability'.	1581379200000	CVE-2020-0660	2
Low	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.36, prior to 6.0.16 and prior to 6.1.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	1579046400000	CVE-2020-2681	1
Low	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure	1578960000000	CVE-2020-0608	1

Severity	Title	Published	CVE	Count
	Vulnerability'.			
Medium	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 and prior to 6.1.12. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).	1594771200000	CVE-2020-14646	1
Medium	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 and prior to 6.1.12. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N).	1594771200000	CVE-2020-14648	1
Medium	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.36, prior to 6.0.16 and prior to 6.1.2. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).	1579046400000	CVE-2020-2701	1
Medium	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.36, prior to 6.0.16 and prior to 6.1.2. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	1579046400000	CVE-2020-2674	1
Medium	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.36, prior to 6.0.16 and prior to 6.1.2. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	1586908800000	CVE-2020-2742	1