

Vulnerabilities report

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

🕒 2020-10-06T03:45:05 to 2020-10-06T09:45:05

🔍 manager.name: dhsiem.verse.in AND rule.groups: vulnerability-detector AND agent.name : "RENT-ARP-LT6004"

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
056	RENT-ARP-LT6004	169.254.27.119	Wazuh v3.13.1	dhsiem.verse.in	Microsoft Windows 10 Pro 10.0.19041	2020-09-04 11:17:47	2020-10-06 04:14:14

Top 3 agents with medium severity vulnerabilities

ID	Name	IP	Version	Manager	OS	Registration date	Last keep alive
056	RENT-ARP-LT6004	169.254.27.119	Wazuh v3.13.1	dhsiem.verse.in	Microsoft Windows 10 Pro 10.0.19041	2020-09-04 11:17:47	2020-10-06 04:14:14

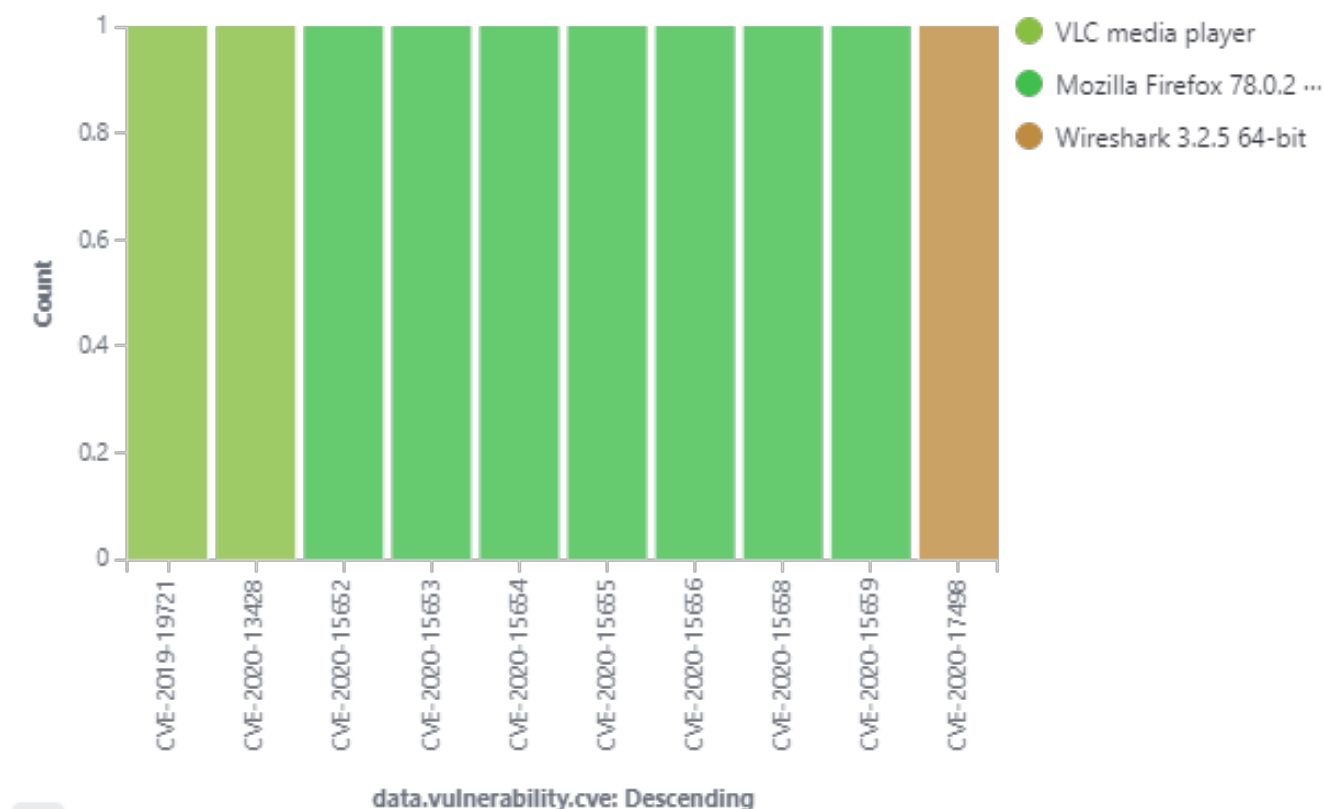
Top 3 CVE

Top	CVE
1	CVE-2019-19721
2	CVE-2020-13428
3	CVE-2020-15652

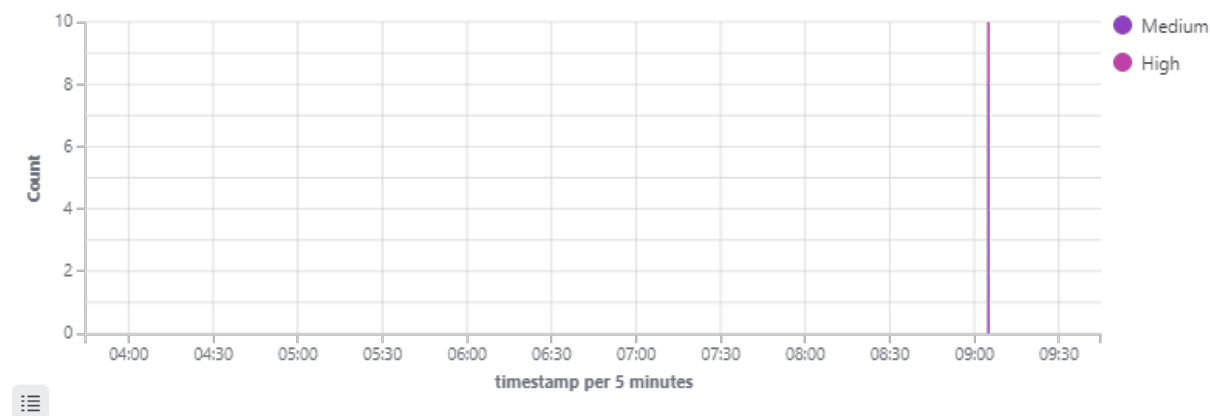
Agents by severity



Top affected packages by CVEs



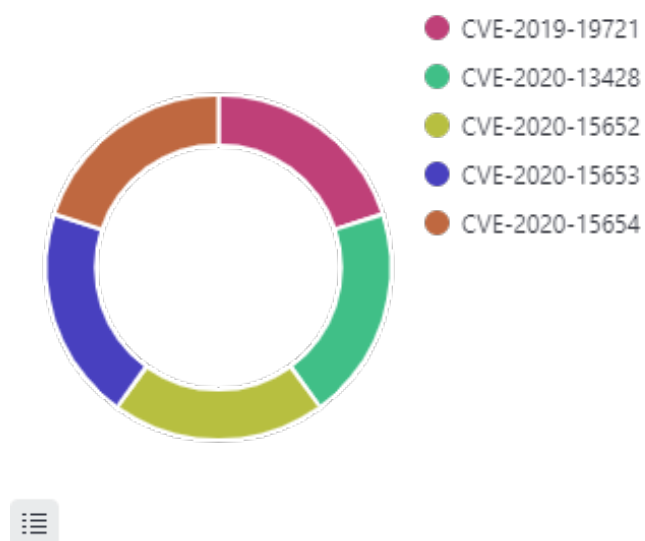
Severity count



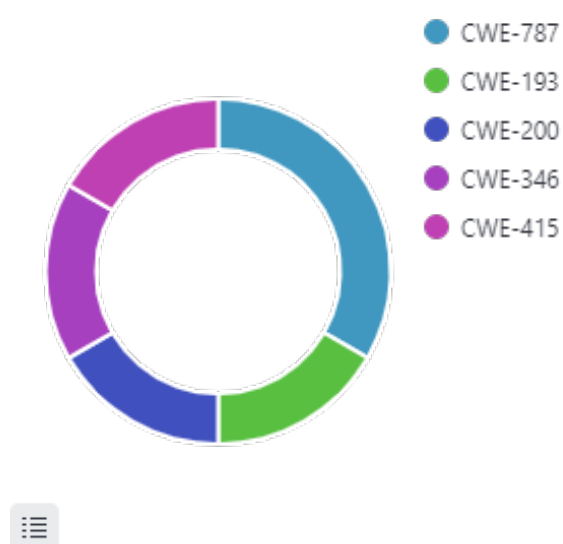
Most affected agents



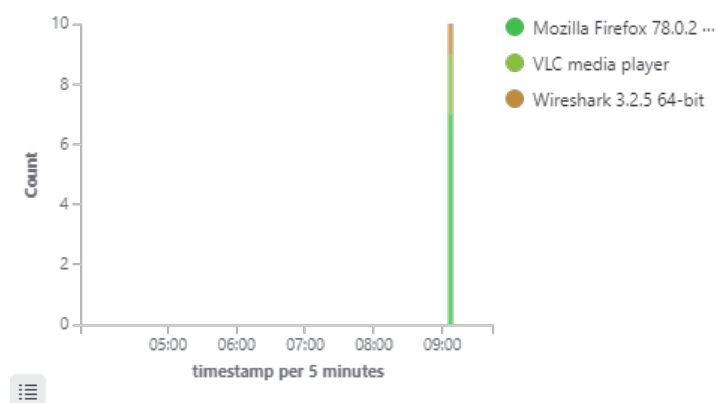
Most common CVEs



Most common CWEs



TOP affected packages alerts Evolution



Alert summary

Severity	Title	Published	CVE	Count
High	JIT optimizations involving the Javascript arguments object could confuse later optimizations. This risk was already mitigated by various precautions in the code, resulting in this bug rated at only moderate severity. This vulnerability affects Firefox ESR < 78.1, Firefox < 79, and Thunderbird < 78.1.	1597017600000	CVE-2020-15656	1
High	Mozilla developers and community members reported memory safety bugs present in Firefox 78 and Firefox ESR 78.0. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 79, Firefox ESR < 68.11, Firefox ESR < 78.1, Thunderbird < 68.11, and Thunderbird < 78.1.	1597017600000	CVE-2020-15659	1
Medium	A heap-based buffer overflow in the hxxx_AnnexB_to_xVC function in modules/packetizer/hxxx_nal.c in VideoLAN VLC media player before 3.0.11 for macOS/iOS allows remote attackers to cause a denial of service (application crash) or execute arbitrary code via a crafted H.264 Annex-B video (.avi for example) file.	1591574400000	CVE-2020-13428	1
Medium	A redirected HTTP request which is observed or modified through a web extension could bypass existing CORS checks, leading to potential disclosure of cross-origin information. This vulnerability affects Firefox ESR < 78.1, Firefox < 79, and Thunderbird < 78.1.	1597017600000	CVE-2020-15655	1
Medium	An iframe sandbox element with the allow-popups flag could be bypassed when using noopener links. This could have led to security issues for websites relying on sandbox configurations that allowed popups and hosted arbitrary content. This vulnerability affects Firefox ESR < 78.1, Firefox < 79, and Thunderbird < 78.1.	1597017600000	CVE-2020-15653	1
Medium	An off-by-one error in the DecodeBlock function in codec/sdl_image.c in VideoLAN VLC media player before 3.0.9 allows remote attackers to cause a denial of service (memory corruption) via a crafted image file. NOTE: this may be related to the SDL_Image product.	1589500800000	CVE-2019-19721	1
Medium	By observing the stack trace for JavaScript errors in web workers, it was possible to leak the result of a cross-origin redirect. This applied only to content that can be parsed as script. This vulnerability affects Firefox < 79, Firefox ESR < 68.11, Firefox ESR < 78.1, Thunderbird < 68.11, and Thunderbird < 78.1.	1597017600000	CVE-2020-15652	1