

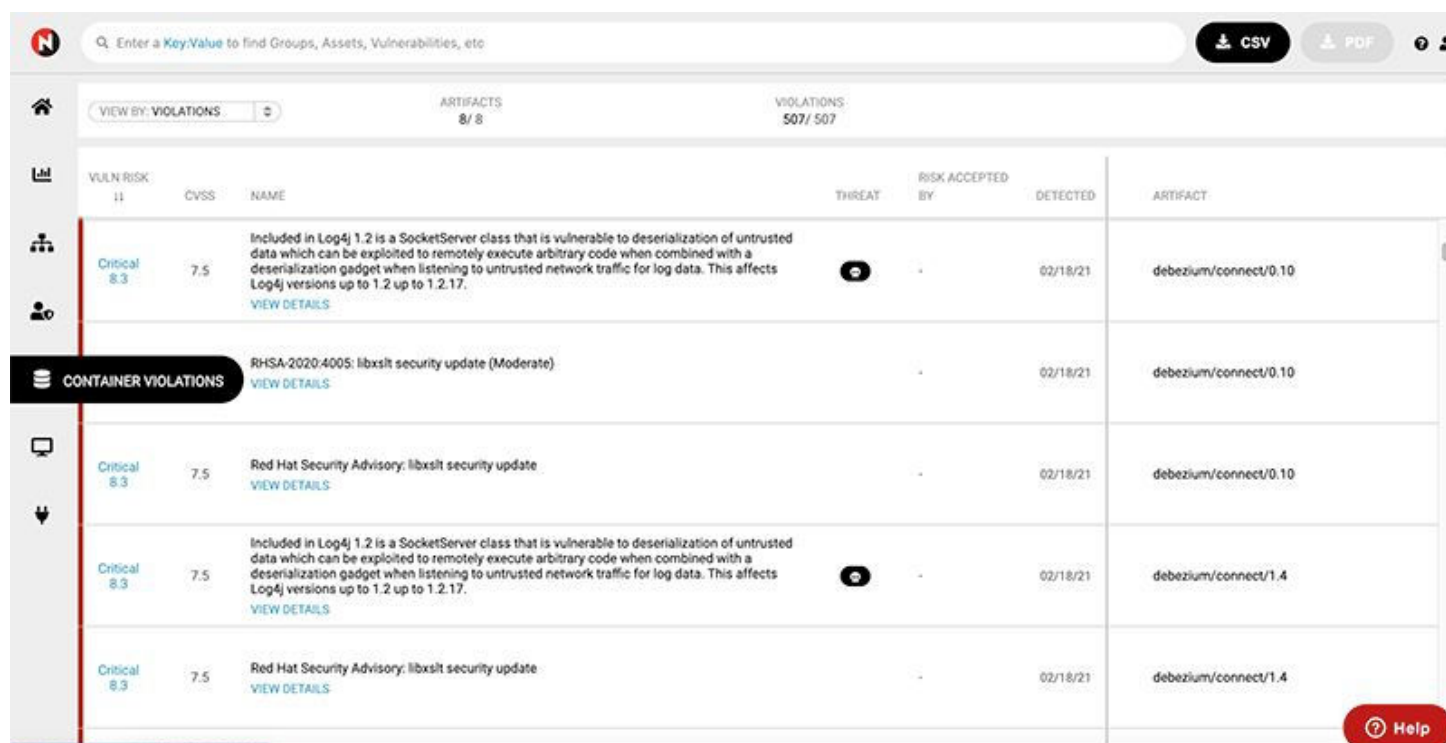
NopSec RBVM Containers Module

Minimize your attack surface by ingesting container configuration and vulnerability scan data to prioritize fixes in your digital artifacts before they get run as images.



Remediate Vulnerabilities within Your Containers

Containers bring a great deal of flexibility to your environment. You can spin instances up off of a master image in minutes — saving time and effort. But, if your master image contains any vulnerabilities, that means you're spinning up duplicate exploit opportunities for anyone looking. Fixing vulnerabilities at the individual instance level just leaves you with more work... And means you could be missing instances that also have that same vulnerability.

NopSec RBVM Containers module enables you to track and remediate vulnerabilities inside your containers. NopSec also tracks any images spun off from that particular container so that you can remediate any active vulnerabilities. By combining your container vulnerability data alongside your infrastructure and application vulnerabilities, you can enable your team to aggregate your prioritization, remediation, and report efforts into one single-source console.



The screenshot shows the NopSec RBVM Containers module interface. At the top, there is a search bar with the placeholder text "Enter a Key/Value to find Groups, Assets, Vulnerabilities, etc". To the right of the search bar are buttons for "CSV", "PDF", and a user profile icon. Below the search bar, there is a "VIEW BY: VIOLATIONS" dropdown menu. To the right of the dropdown are two counters: "ARTIFACTS 8/8" and "VIOLATIONS 507/ 507". The main table displays a list of vulnerabilities. The table has columns for "VULN RISK", "CVSS", "NAME", "THREAT", "RISK ACCEPTED BY", "DETECTED", and "ARTIFACT". The first row shows a "Critical" risk with a CVSS score of 7.5, related to Log4j 1.2, detected on 02/18/21, and associated with the artifact "debezium/connect/0.10". A "CONTAINER VIOLATIONS" sidebar is visible on the left, and a "Help" button is in the bottom right corner.

VULN RISK	CVSS	NAME	THREAT	RISK ACCEPTED BY	DETECTED	ARTIFACT
Critical 8.3	7.5	Included in Log4j 1.2 is a SocketServer class that is vulnerable to deserialization of untrusted data which can be exploited to remotely execute arbitrary code when combined with a deserialization gadget when listening to untrusted network traffic for log data. This affects Log4j versions up to 1.2 up to 1.2.17. VIEW DETAILS		-	02/18/21	debezium/connect/0.10
CONTAINER VIOLATIONS						
		RHSA-2020-4005: libxslt security update (Moderate) VIEW DETAILS			02/18/21	debezium/connect/0.10
Critical 8.3	7.5	Red Hat Security Advisory: libxslt security update VIEW DETAILS			02/18/21	debezium/connect/0.10
Critical 8.3	7.5	Included in Log4j 1.2 is a SocketServer class that is vulnerable to deserialization of untrusted data which can be exploited to remotely execute arbitrary code when combined with a deserialization gadget when listening to untrusted network traffic for log data. This affects Log4j versions up to 1.2 up to 1.2.17. VIEW DETAILS		-	02/18/21	debezium/connect/1.4
Critical 8.3	7.5	Red Hat Security Advisory: libxslt security update VIEW DETAILS			02/18/21	debezium/connect/1.4

NopSec helps security professionals simplify their work, effectively manage and prioritize vulnerabilities, and make better informed decisions. NopSec's Unified VRM is an innovative threat and vulnerability management solution that addresses the need for better prioritization and remediation of security vulnerabilities in a single platform.