How to scan your Windows and Linux applications for log4j vulnerabilities with Runecast Analyzer

Runecast is committed to helping our customers stay secure and discovering vulnerable Log4j instances in their Windows and Linux applications.

Our development team has worked tirelessly to update the Runecast platform for our clients to counter the Log4Shell vulnerability. This now includes the ability to scan your Operating Systems (OS) to find vulnerabilities. Anybody using Java framework applications is likely to be vulnerable to one of the biggest and most severe vulnerabilities.

Contents

1. How to deploy Runecast Analyzer

Before any scanning can take place Runecast Analyzer must be deployed in your infrastructure. To find the complete steps to deploy it on VMware, AWS or Azure please consult the deployment guide. Runecast Analyzer is typically deployed in minutes as a pre-installed, pre-configured virtual machine.

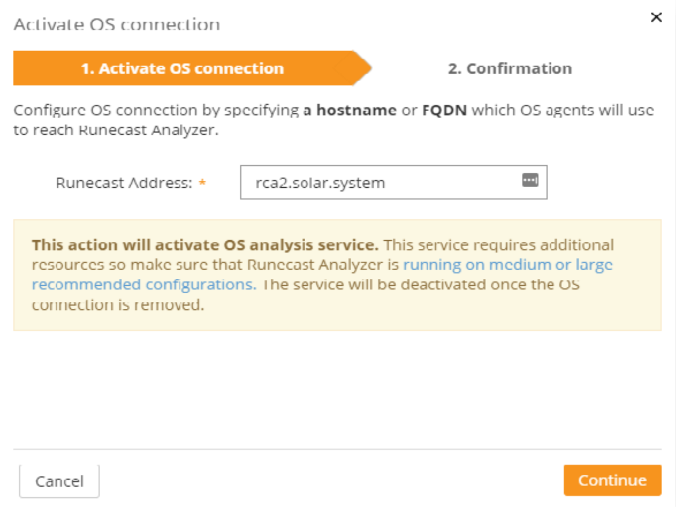
With one Runecast Analyzer instance you can scan your entire estate across multiple platforms and devices. The Analyzer doesn’t upload any information outside of your organization and can run in dark sites.

2. How to enable OS Analysis

To enable Operating Systems (OS) Analysis, navigate to Settings, in the Connections tab and click on the Activate OS Connection button.

Enter the hostname, FQDN or IP Address, that will be used by the OS agents to access Runecast Analyzer, and press Continue. This is effectively the IP or FQDN of your Runecast Analyzer instance.

Once this is complete you will be presented with confirmation that the OS analysis service was enabled.
Press Finish to confirm. You will then find the Operating Systems on the Connections page.



Activate OS connection

Configure OS connection by specifying **a hostname** or **FQDN** which OS agents will use to reach Runecast Analyzer.

Runecast Address: * rca2.solar.system

This action will activate OS analysis service. This service requires additional resources so make sure that Runecast Analyzer is running on medium or large recommended configurations. The service will be deactivated once the OS connection is removed.

3. How to deploy OS Agents for Runecast Analyzer

Runecast Analyzer uses lightweight and secure agents to obtain the necessary data from the Windows and Linux instances you want to analyze. You can deploy the agents manually or automatically. Runecast recommends using an automated deployment where possible.

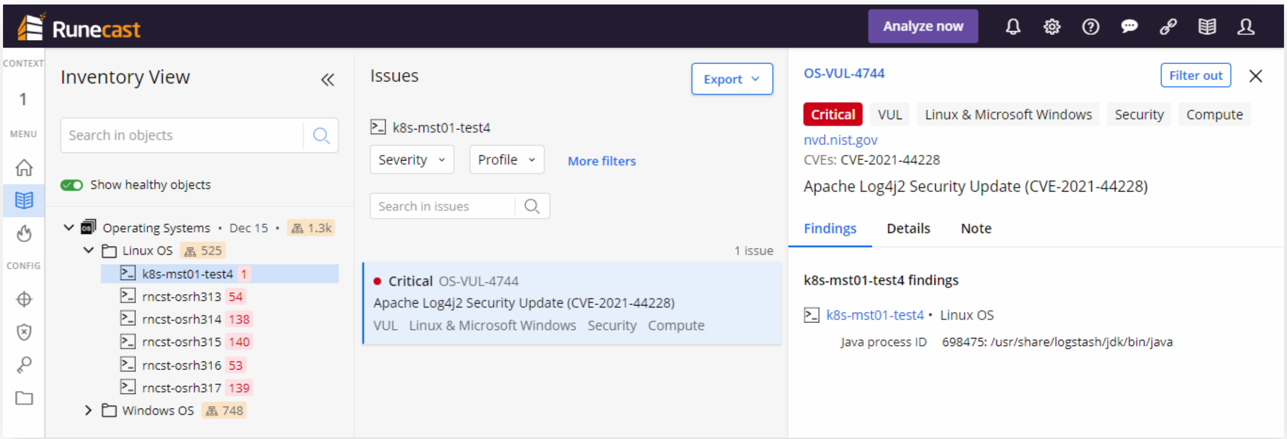
In the Runecast Analyzer deployment instructions there are two examples of how to perform automatic deployment of agents. One on Linux, using Ansible, and one on Windows with Active Directory Group Policy.

Please note: the Runecast OS Agents leverage a highly secure and industry-proven agent called osquery. This lightweight and easy to deploy agent means there's no need for SSH or other less secure methods of obtaining information from your Operating Systems. In addition, Runecast Analyzer has full offline capabilities and doesn't send any data out of your network. You can rest assured that your data is safe when you're using Runecast.

4. How to analyze and discover log4j vulnerabilities

Once Runecast Analyzer's OS agents are deployed, click Analyze now.

Once the analysis is complete, select the Inventory View on the left hand menu and search for log4j. This will highlight any instances of the log4j library that are vulnerable, as shown below.



Operating Systems • Dec 15 • 1.3k
Linux OS 525
k8s-mst01-test4 1
rncst-osrh313 54
rncst-osrh314 138
rncst-osrh315 140
rncst-osrh316 53
rncst-osrh317 139
Windows OS 748

k8s-mst01-test4

1 issue

● Critical OS-VUL-4744
Apache Log4j2 Security Update (CVE-2021-44228)
VUL Linux & Microsoft Windows Security Compute

OS-VUL-4744

Critical VUL Linux & Microsoft Windows Security Compute
nvd.nist.gov
CVEs: CVE-2021-44228
Apache Log4j2 Security Update (CVE-2021-44228)

k8s-mst01-test4 findings

k8s-mst01-test4 • Linux OS

Java process ID 698475: /usr/share/logstash/jdk/bin/java