CVE Number, Company, Product, ...

○ By Relevance ○ By Risk Score ○ By Publish Date ○ By Recent Activity

CVE-2021-3762 quay/claircore: directory traversal when scanning crafted container image

Related Vulnerabilities: CVE-2021-3762

🔗 Source

```
        Hello,

A directory traversal vulnerability was found in the ClairCore engine of
Clair.
An attacker can exploit this by supplying a crafted container image which,
when scanned by Clair, allows for arbitrary file write on the filesystem,
potentially allowing for remote code execution.

Red Hat has assigned CVE-2021-3762 to this vulnerability.
These issues have been rated Critical, with a CVSS:
9.8CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

### Affected Versions
ClairCore 0.4.6 release and higher (Clair v4.1.4 and higher)
ClairCore 0.5.3 release and higher (Clair v4.2.1 and higher)

### Fixed Versions
ClairCore v0.4.8 (shipped in Clair v4.1.6)
ClairCore v0.5.5 (shipped in Clair v4.2.3)

### Fixes
https://github.com/quay/claircore/pull/478
https://github.com/quay/clair/pull/1379
https://github.com/quay/clair/pull/1380

## Acknowledgements
Yanir Tsarimi
twitter.com/Yanir_
(Orca Security)


Best regards,
Przemyslaw Roguski

--
Przemyslaw Roguski / Red Hat Product Security
```

About

About
Home
Recent Vulnerabilities
Research Posts
Trends
Blog
About
Contact

Products

Vulmon Search
Vulmon Research
Vulmon Alerts
Vulmap

Connect

Twitter
Reddit
Linkedin
Facebook

Vulnerability Notification Service

You don't have to wait for vulnerability scanning results

Get Started