# CVE Detail – CVE-2021-21272

ORAS is open source software which enables a way to push OCI Artifacts to OCI Conformant registries. ORAS is both a CLI for initial testing and a Go Module. In ORAS from version 0.4.0 and before version 0.9.0, there is a "zip-slip" vulnerability. The directory support feature allows the downloaded gzipped tarballs to be automatically extracted to the user-specified directory where the tarball can have symbolic links and hard links. A well-crafted tarball or tarballs allow malicious artifact providers linking, writing, or overwriting specific files on the host filesystem outside of the user-specified directory unexpectedly with the same permissions as the user who runs `oras pull`. Users of the affected versions are impacted if they are `oras` CLI users who runs `oras pull`, or if they are Go programs, which invoke `github.com/deislabs/oras/pkg/content.FileStore`. The problem has been fixed in version 0.9.0. For `oras` CLI users, there is no workarounds other than pulling from a trusted artifact provider. For `oras` package users, the workaround is to not use `github.com/deislabs/oras/pkg/content.FileStore`, and use other content stores instead, or pull from a trusted artifact provider.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.44993

## CVSS Scoring

CVSS v3.1 Score: 7.7

Severity: HIGH

## Mapped CWE(s)

* CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
* CWE-59: Improper Link Resolution Before File Access ('Link Following')

## CAPEC(s)

* CAPEC-126: Path Traversal
* CAPEC-132: Symlink Attack
* CAPEC-17: Using Malicious Files
* CAPEC-35: Leverage Executable Code in Non-Executable Files
* CAPEC-64: Using Slashes and URL Encoding Combined to Bypass Validation Logic
* CAPEC-76: Manipulating Web Input to File System Calls
* CAPEC-78: Using Escaped Slashes in Alternate Encoding
* CAPEC-79: Using Slashes in Alternate Encoding

## ATT&CK Techniques

* T1027.009: Embedded Payloads
* T1547.009: Shortcut Modification
* T1574.005: Executable Installer File Permissions Weakness
* T1574.010: Services File Permissions Weakness
* T1564.009: Resource Forking
* T1027.006: HTML Smuggling

## Used By (Actors/Tools)

* Pikabot (malware)
* RedLeaves (malware)
* macOS.OSAMiner (malware)
* EnvyScout (malware)
* SslMM (malware)
* Emotet (malware)
* DUSTTRAP (malware)
* BADHATCH (malware)
* DUSTPAN (malware)
* Moneybird (malware)
* InvisiMole (malware)
* Keydnap (malware)
* Okrum (malware)
* IcedID (malware)
* MarkiRAT (malware)
* Kazuar (malware)
* CHIMNEYSWEEP (malware)
* BlackEnergy (malware)
* Reaver (malware)
* MultiLayer Wiper (malware)
* S-Type (malware)
* SeaDuke (malware)
* Netwalker (malware)
* Gazer (malware)
* SMOKEDHAM (malware)
* Uroburos (malware)
* KONNI (malware)
* SPACESHIP (malware)
* Micropsia (malware)
* RogueRobin (malware)
* Grandoreiro (malware)
* Bazar (malware)
* SHIPSHAPE (malware)
* TinyZBot (malware)
* DEADEYE (malware)
* FELIXROOT (malware)
* ComRAT (malware)
* Astaroth (malware)
* QakBot (malware)
* Helminth (malware)
* OSX/Shlayer (malware)
* DEADWOOD (malware)
* Comnie (malware)
* Dtrack (malware)
* BACKSPACE (malware)
* Empire (tool)
* Invoke-PSImage (tool)
* Lazarus Group (intrusion-set)
* TA577 (intrusion-set)
* APT29 (intrusion-set)
* APT39 (intrusion-set)
* Leviathan (intrusion-set)
* Gorgon Group (intrusion-set)
* C0021 (campaign)
* Moonstone Sleet (intrusion-set)

## Affected Products

* cpe:2.3:a:deislabs:oras:\*:\*:\*:\*:\*:\*:\*:\*