containers / podman Public

Code Issues 939 Pull requests 154 Discussions Actions Projects

PowerShell Command Injection in Podman HyperV Machine

Low **Luap99** published **GHSA-hc8w-h2mf-hp59** 10 hours ago

Package

github.com/containers/podman (Go)

Affected versions

>= v4.8.0, <= v5.8.1

Patched versions

v5.8.2

Description

Summary

A command injection vulnerability exists in Podman's HyperV machine backend. The VM image path is inserted into a PowerShell double-quoted string without sanitization, allowing `$()` subexpression injection.

Affected Code

File: `pkg/machine/hyperv/stubber.go:647`

```
resize := exec.Command("powershell", []string{
    "-command",
    fmt.Sprintf("Resize-VHD \"%s\" %d", imagePath.GetPath(), newSize.ToBytes()),
}...)
```

Root Cause

PowerShell evaluates `$()` subexpressions inside double-quoted strings before executing the outer command. The `fmt.Sprintf` call places the user-controlled image path directly into double quotes without escaping or sanitization.

Impact

An attacker who can control the VM image path (through a crafted machine name or image directory) can execute arbitrary PowerShell commands with the privileges of the Podman process on the Windows host. On typical Windows installations, this means SYSTEM-level code execution.

Patch

`571c842`

The affected code is only used on Windows, all other operating systems are not affected by this and can thus ignore the CVE patch.

Credit

We like to thank Sang-Hoon Choi (**@KoreaSecurity**) for reporting this issue to us.

Severity

Low

CVE ID

CVE-2026-33414

Weaknesses

▶ CWE-78

Credits

KoreaSecurity Reporter