# Discovered a new zero-day vulnerability on macOS that allows attackers to run commands remotely

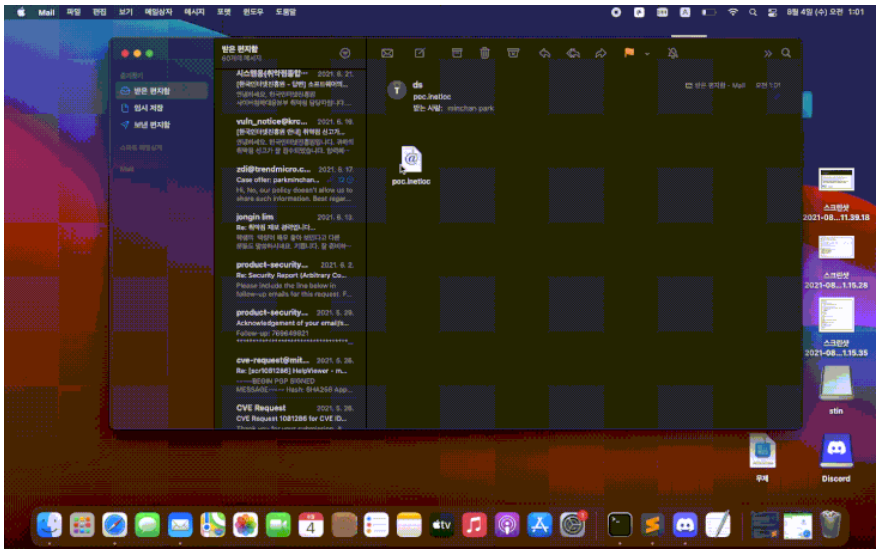
An international team of security researchers has publicly disclosed a new vulnerability that exists in Apple's macOS Finder.

This is essentially a high-severity zero-day vulnerability that could allow an attacker to execute arbitrary commands on a target Mac, regardless of the version of macOS in use.

This vulnerability was first found by a team of independent security researchers led by cybersecurity expert Park Minchan. The problem stems from the way macOS handles inetloc files, which inadvertently causes the system to automatically run any commands embedded inside by the attacker without being able to issue any warnings or prompts. for users.

On macOS, Internet location files with the .inetloc extension are system-wide storage of bookmark data, and can be used to open online resources (news://, ftp://) , afp://) or local files (file://).

> "A vulnerability in macOS Finder allows files with the inetloc extension to execute arbitrary commands. These files could be embedded inside malicious email messages that, if clicked by the user, would immediately execute the commands specified. embedded inside without giving any prompts or warnings to the user'.



For its part, Apple seems to be aware of the problem and is quietly fixing it without specifying a CVE identifier. The Park Minchan team and colleagues also discovered that Apple's patch only partially addresses the vulnerability, as it can still be exploited by changing the protocol used to execute embed commands from the

file. :// to File://.

> "We have informed Apple that FiLe:// (value change only) does not appear to be blocked, but have not received any response from them so far. As far as we know, currently Currently, this vulnerability has not really been patched."

The team has not provided any specific information on how attackers can abuse this vulnerability. However, in theory, it is entirely possible to be used by threat actors to create malicious email attachments that can launch an accompanying or remote payload when accessed by the victim.

Initial field tests have confirmed that this vulnerability can be used to run arbitrary commands on macOS Big Sur, using specially crafted files downloaded from the Internet without any any prompts or warnings.

A .inetloc file with PoC code also went undetected by any anti-malware engine on VirusTotal. That means macOS users targeted by threat actors using this attack method will not be protected by security software.

Hopefully Apple will soon implement more thorough measures to fix the problem in the near future

You finished reading the article "**Discovered a new zero-day vulnerability on macOS that allows attackers to run commands remotely**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

---

© 2019 TipsMake.com