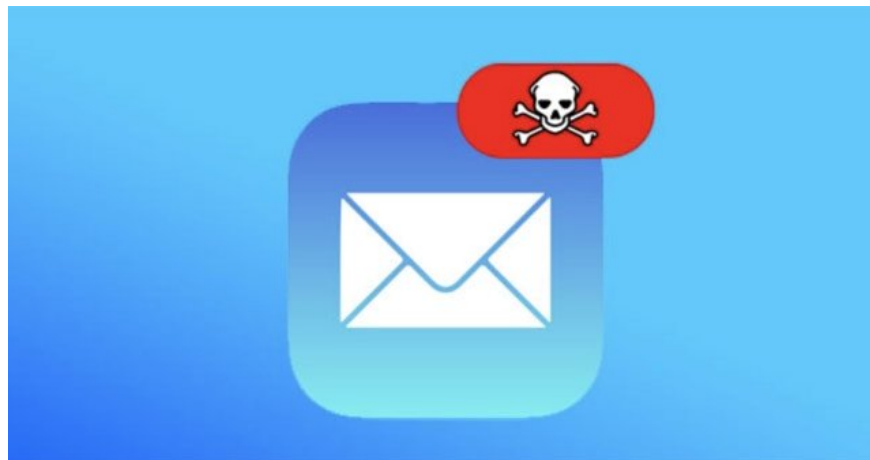


The Mail app on iOS has serious vulnerabilities

Security researchers at ZecOps have discovered two serious vulnerabilities that exist on the default Mail application pre-installed on millions of iPhones and iPads.

Security researchers at ZecOps have discovered two serious vulnerabilities that exist on the default Mail application pre-installed on millions of iPhones and iPads.

These two vulnerabilities are related to out-of-bound write and remote heap overflow in the MIME library of the Mail application. The vulnerability allows hackers to remotely execute code and infect the device by sending emails consuming large amounts of RAM to any individual whose email account is logged into the Mail application. Full control of Apple devices.



In particular, the vulnerability associated with buffer overflow is more dangerous because it does not require interaction from the recipient.

Both of these vulnerabilities have existed for the past 8 years, since iOS 6 launched and they still affect the latest version of iOS 13.4.1.

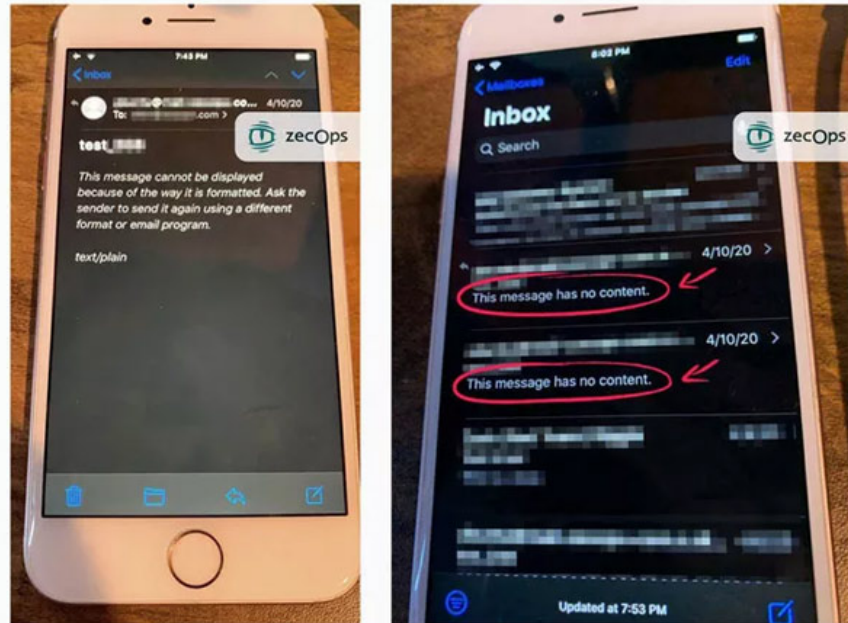
More worrying is that many attackers have been exploiting these vulnerabilities to track victims, at least for the past two years. At least 6 organizations have been affected by this hole.

According to the researchers, after remotely accessing the victim's device, the attacker immediately deletes the malicious email, making it difficult for Apple users to detect.

After successfully exploiting this vulnerability, hackers will run a malicious code to "leak, modify and delete emails". For complete control of the device remotely, an attacker needs to connect it to a separate kernel vulnerability in the system.

Attacking iOS Devices through MobileMail/Maild

Failed attack looks like this:



ZecOps discovered these two vulnerabilities almost two months ago and reported it to Apple.

Up to now, the security patches to fix both these vulnerabilities have only appeared on the iOS 13.4.5 beta version released by Apple last week.

Apple will soon release a software patch in the upcoming iOS update for general iPhone and iPad users. From now until patch is available, it is best to use Outlook or Gmail instead of the built-in email application.

You finished reading the article "**The Mail app on iOS has serious vulnerabilities**" 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.