Detecting extremely serious vulnerabilities that allow hacking iPhone just by sending email, victims who are not open are also attacked

The default email client pre-installed on millions of iPhones and iPads now has two serious vulnerabilities that hackers can exploit to silently gain control of remote devices through sending email to users.

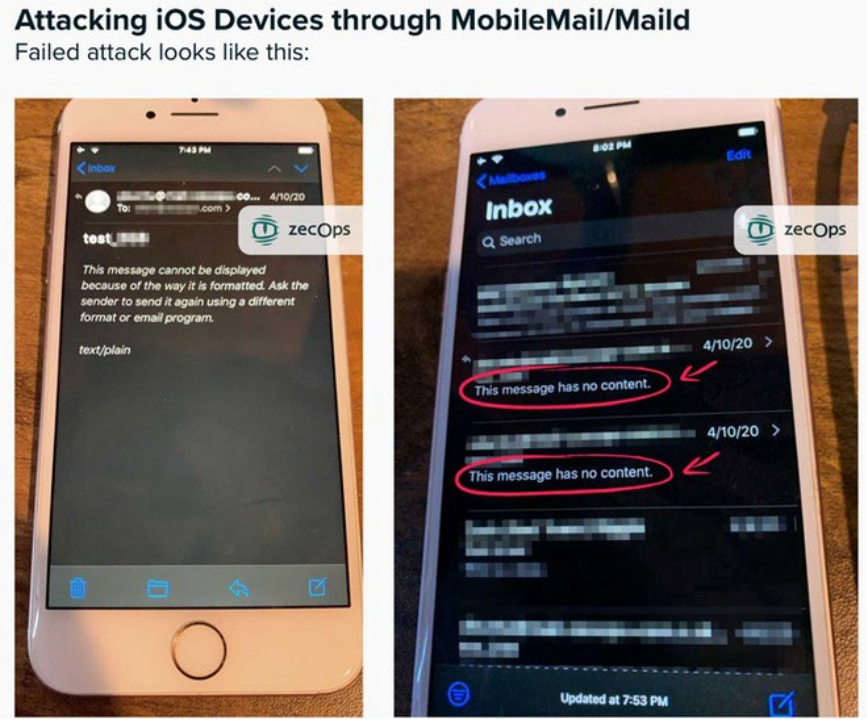
According to cybersecurity researchers at ZecOps, the aforementioned vulnerabilities are related to out-of-bound write and remote heap overflow, one of which is the " zero-click "extremely dangerous, can be taken advantage of without any interaction from people who receive email.

Both remote code execution errors that are located in the email client's MIME library can be triggered while processing email content. These errors have existed for the past 8 years, since iOS 6 was released, and affect the latest iOS 13.4.1.

More worrying is that many hacker groups have been taking advantage of these errors for at least the past 2 years to target individual users working in various fields and organizations, MSSP different from Saudi Arabia. Saudi and Israel, to journalists in Europe.

" *With a very limited amount of data, we were able to see at least 6 organizations affected by this vulnerability - and the scale of the impact was extremely large,* " the researchers said. .

" *Although ZecOps has not yet confirmed that these attacks have been carried out by a specific individual, we are aware that at least one 'mercenary hacker' organization is selling tools that take advantage of related vulnerabilities. email address* ".



According to the researchers, it is difficult for Apple users to know whether they have been targeted by other cyber attacks, because hackers immediately deleted the malicious email after gaining remote access. victim's device.

"It is worth noting that, although the data confirming that the abused emails were received and processed by the victim's iOS device, the corresponding emails that should have been received and stored on the email server disappear. Therefore, we anticipate that these emails were intentionally deleted as part of the site cleanup plan after an attack, "the researchers said.

" *In addition to a temporary slowing down of the mobile email application, users will not observe any other unusual behavior* ."

After successfully exploiting the flaw, the hacker will run a malicious code alongside the MobileMail or Maild application, allowing them to " *leak, edit, and delete emails* ". However, to take full control of the device remotely, a hacker needs to combine it with another security hole in the system kernel.

ZecOps discovered the above vulnerabilities and attacks almost two months ago and reported it to Apple's security team.

So far, only the iOS 13.4.5 beta version that was released last week contains other security patches that address both of these zero-day vulnerabilities.

For iPhone and iPad users in general, they will soon receive a software patch in the upcoming iOS update. But in the meantime, it's best not to use the built-in email app, instead use Outlook or Gmail.