Google has just patched a critical Gmail vulnerability, allowing hackers to send fake emails

Google just patched a critical vulnerability affecting Gmail and G Suite. This vulnerability allows hackers to send fake identity emails to scam users.

Security researcher Allison Husain is the one who discovered a Gmail security vulnerability that Google has just fixed. According to Husain, the cause of the problem lies in the lack of a verification mechanism when configuring email routes.

"Both Gmail and G Suite's strict DMARC / SPF policy can be circumvented by using G Suite mail routing rules to forward and grant authentication to spoofed emails , " says Husain. shall.

Husain discovered the problem in early 2020 and reported it to Google on 3/4/2020. Google took over the issue on April 16, 2020 but later determined that the vulnerability was prioritized only at level 2, severity level 2, and then marked it as a duplicate vulnerability. .

Google delayed patching the vulnerability by 137 days and would only patch it when it went public on the internet

When Husain informed Google that he would make the vulnerability public on August 17, Google said a patch was under development and expected to roll out on September 17. According to Google regulations, the vulnerability will be patched within 90 days from when it is reported to Google and after this deadline a developer can publicize the vulnerability they discover. In the case of Husain, the Gmail vulnerability has not been patched even though it was reported 137 days ago.

Therefore, Husain decided to publicize the vulnerability on August 19 to promote Google to quickly take measures to protect users. Husain's decisive action forced Google to immediately take corrective measures.

Within 7 hours of Husain published details of the vulnerability, Google has released a patch.