

NCSA OpenSource Emails

As some of you might have noticed the confluence server started to send out emails with an invalid FROM header as well as a prefix to the subject. The emails would have "Actividad sospechosa detectada" added to the subject header as well as made it look like they came from "Soporte BBVA Colombia <someemail>". These emails did indeed originate from confluence, but the outgoing email address of confluence was modified.

Once this was brought to our light we immediately started to work with the NCSA security team to investigate this incident. We have discovered how this was done and have mitigated the issue. We are currently investigating if anything else was modified, however we not discovered any other modifications done. We will continue to work with the security team as well as do a more thorough investigation of what this user accessed. If we discover anything specific we will contact those projects and people affected.

These changes were made on September 27th 2018, at around 5:30pm central time. We undid these changes September 28th at around 11:00am central time.