Facebook admits storing millions of passwords in readable plain text

23/03/2019 13:36 by admin

Facebook left hundreds of millions of user passwords readable by its employees for years, the company acknowledged Thursday after a security researcher exposed the lapse.

San Fransisco: Facebook left hundreds of millions of user passwords readable by its employees for years, the company acknowledged Thursday after a security researcher exposed the lapse .

By storing passwords in readable plain text, Facebook violated fundamental computer-security practices. Those call for organizations and websites to save passwords in a scrambled form that makes it almost impossible to recover the original text.

â€œThere is no valid reason why anyone in an organization, especially the size of Facebook, needs to have access to usersâ€™ passwords in plain text,â€• said cybersecurity expert Andrei Barysevich of Recorded Future.

Facebook said there is no evidence its employees abused access to this data. But thousands of employees could have searched them. The company said the passwords were stored on internal company servers, where no outsiders could access them. Even so, some privacy experts suggested that users change their Facebook passwords.

The incident reveals yet another huge and basic oversight at a company that insists it is a responsible guardian for the personal data of its 2.3 billion users worldwide.

The security blog KrebsOnSecurity said Facebook may have left the passwords of some 600 million Facebook users vulnerable. In a blog post , Facebook said it will likely notify â€œhundreds of millionsâ€• of Facebook Lite users, millions of Facebook users and tens of thousands of Instagram users that their passwords were stored in plain text.

Facebook Lite is a version designed for people with older phones or low-speed internet connections. It is used primarily in developing countries.

Last week, Facebook CEO Mark Zuckerberg touted a new â€•privacy-focused vision â€• for the social network that would emphasize private communication over public sharing. The company wants to encourage small groups of people to carry on encrypted conversations that neither Facebook nor any other outsider can read.

The fact that the company couldnâ€™t manage to do something as simple as encrypting passwords, however, raises questions about its ability to manage more complex encryption issues â€” such in messaging â€” flawlessly.

Facebook said it discovered the problem in January. But security researcher Brian Krebs wrote that in some cases the passwords had been stored in plain text since 2012. Facebook Lite launched in 2015 and Facebook bought Instagram in 2012.

The problem, according to Facebook, wasnâ€™t due to a single bug. During a routine review in January, it say, it found that the plain text passwords were unintentionally captured and stored in its internal storage systems. This happened in a variety of circumstances â€” for example, when an app crashed and the resulting crash log included a captured password.

But Alex Holden, the founder of Hold Security, said Facebookâ€™s explanation is not an excuse for sloppy security practices that allowed so many passwords to be exposed internally.

Recorded Futureâ€™s Barysevich said he could not recall any major company caught leaving so many passwords exposed. He said heâ€™s seen a number of instances where much smaller organizations made such information readily available â€” not just to programmers but also to customer support teams.

Security analyst Troy Hunt, who runs the â€œhaveibeenpwned.comâ€• data breach website , said the situation may be embarrassing for Facebook but not dangerous unless an adversary gained access to the passwords. Facebook has had major breaches, most recently in September when attackers accessed some 29 million accounts .

Jake Williams, president of Rendition Infosec, said storing passwords in plain text is â€œunfortunately more common than most of the industry talks aboutâ€• and tends to happen when developers are trying to rid a system of bugs.

He said the Facebook blog post suggests storing passwords in plain text may have been â€œa sanctioned practice,â€• although he said itâ€™s also possible a â€œrogue development teamâ€• was to blame.

Hunt and Krebs both likened Facebookâ€™s failure to similar stumbles last year on a far smaller scale at Twitter and GitHub; the latter is a site where developers store code and track projects. In those cases, software bugs were blamed for accidentally storing plaintext passwords in internal logs.

Facebookâ€™s normal procedure for passwords is to store them encoded, the company noted Thursday in its blog post.

Thatâ€™s good to know, although Facebook engineers apparently added code that defeated the safeguard, said security researcher Rob Graham. â€œThey have all the proper locks on the doors, but somebody left the window open,â€• he said.

- AP