Data breach at Weebly affects 43 million users

grahamcluley.com/data-breach-weebly-affects-43-million-users/

10/23/2016

A data breach at free website builder Weebly has compromised the personal information of over 43 million users.

News of the breach arrived on 20 October when LeakedSource.com published a database of 43,430,316 Weebly users' information on its website. Those records contain a username, email address, password, and IP address.

Little information is known about how those responsible for the breach exfiltrated all of that data, but we do know that the breach occurred at the web-hosting service in February 2016 and that an anonymous source provided LeakedSource with the database.

LeakedSource says the breach could have been much worse had Weebly's teams not implemented an important security feature:

> *"This mega breach affects not only tens of millions of users but tens of millions of websites and with Weebly being one of the most popular hosting platforms in the world, this breach could have been far more disastrous in the wrong hands had they not strongly hashed passwords."*

Specifically, Weebly used a salted Bcrypt hash with a factor of 8. LeakedSource reports the security team at the company has bumped that factor up to 10 in order to more securely store users' passwords.

It also appears that Weebly co-founder Chris Fanini is big on communication. He's working with LeakedSource to make sure the company sends out breach notification and password reset emails to all affected users.

Weebly has since confirmed the breach and stated that all of those efforts are now underway. As quoted by *The Hacker News*:

> *"Weebly recently became aware that an unauthorized party obtained email addresses and/or usernames, IP addresses and encrypted (bcrypt hashed) passwords for a large number of customers.*
>
> *"At this point, we do not have evidence of any customer website being improperly accessed. We do not store any full credit card numbers on Weebly servers, and at this time we're not aware that any credit card information that can be used for fraudulent charges was part of this incident."*

In the same release, LeakedSource also shared the news of over 22 million users affected by what they claim was a breach at Foursquare dating from December 2013. Those records are said to contain users' names, usernames, gender, location, Facebook name, and Twitter ID.

ZDNet has verified a number of FourSquare user records provided to it. But in an email, a spokesperson for the location-based check-in site said, "no breach has occurred."

Maybe we would be wise to believe Foursquare in this instance. After all, it appears that the "breached" data that LeakedSource says it has received could have been collated by scraping the Foursquare website for information that users have publicly shared - such as their location and Facebook/Twitter usernames - on their profile pages.

In an ideal world, maybe Foursquare would have prevented attempts to scrape up large amounts of user data via rate-limiting, but unless some information has been collected that *isn't* intentionally shared by users it feels something of a stretch to call this a conventional data breach.

Given all of these recent breaches at LinkedIn, Tumblr, Yahoo, and more, it's important that any user notified of a data breach change their passwords as soon as possible.

All of us need to learn to never reuse their passwords across multiple accounts and to remember to always implement two-step verification (2SV) when it's available.