Hack on Stack Overflow exposes private data for ~250 users



reader comments

15 with 15 posters participating

Share this story

Stack Overflow said hackers obtained private data for about 250 users after breaching the site and spending the next week escalating their access.

“While our overall user database was not compromised, we have identified privileged Web requests that the attacker made that could have returned IP address, names, or emails for a very small number of Stack Exchange users,” Mary Ferguson, Stack

Overflow VP of Engineering, wrote in a blog post published Friday. “Our team is currently reviewing these logs and will be providing appropriate notifications to any users who are impacted.”

In an update, Ferguson said investigators now estimate the number at 250 public network users. Officials for the developer community site will notify those affected. The company first disclosed the breach on Thursday in a four-sentence post that said “some level of production access was gained on May 11.”

In Friday’s update, Ferguson said the intrusion started on May 5, when an attacker exploited a bug in a new build deployed to the development tier of stackoverflow.com. The access allowed the attacker to log into the development tier and then escalate access to a production version of the site. The attacker has since been removed from the network.

“Between May 5 and May 11, the intruder contained their activities to exploration,” Ferguson wrote. “On May 11, the intruder made a change to our system to grant themselves a privileged access on production. This change was quickly identified and we revoked their access network-wide, began investigating the intrusion, and began taking steps to remediate the intrusion.”

To minimize the damage hackers can do, Stack Overflow maintains separate systems for the site’s Teams, Business, and Enterprise customers. So far, investigators have found no evidence that these systems or the customer data belonging to them were access. The company’s advertising and talented business were also not affected, the VP said. Stack Overflow has about 10 million registered users.

Stack Overflow is now in the process of auditing all logs and databases in an attempt to trace the intruder’s steps. It has also fixed the original weaknesses that allowed the intrusion

and escalation to happen. The company has retained a third-party forensics and incident response firm to assist in both remediation and evaluation of systems and security levels. Ferguson said Stack Overflow will provide more information once the investigation concludes.

https://arstechnica.com/?p=1507321