By John Leyden, TheRegister.co.uk

Open-source code repository SourceForge has advised users to change their passwords following a concerted hacking attack.

The attack, launched last Wednesday, targeted developer infrastructure and involved the compromise of SourceForge.net servers. SourceForge detected the attack and quickly disabled CVS, ishell, file uploads, and project web updates as a precaution against deeper compromise.

The open-source outfit reckons it nipped the attack before it got very far. However, analysis of server logs after the attack revealed that an SSH daemon had been modified to carry out a password-sniffing attack.

SourceForge reckons it was unlikely any developer passwords were actually compromised, though it can't be absolutely sure. As a precaution, the open-source site applied an across-the-board password reset, as explained in an email to developers sent over the weekend and forwarded to *El Reg*.

We recently experienced a directed attack on SourceForge infrastructure (https://sourceforge.net/blog/sourceforge-net-attack) and so we are resetting all passwords in the sf.net database – just in case. We're emailing all sf.net registered account holders to let you know about this change to your account.

Our investigation uncovered evidence of password sniffing attempts. We have no evidence to suggest that your password has been compromised. But, what we definitely don't want is to find out in two months that passwords were compromised and we didn't

take action.

So, as a proactive measure we've invalidated your SourceForge.net account password. To access the site again, you'll need to go through the email recovery process and choose a shiny new password.

An update on the SourceForge blog, published on Saturday, provides a detailed update on the attack and SourceForge's response thus far. SourceForge hopes to fully restore services later this week.

It's unclear who carried out the attack or what exactly their motives might have been, although uploading back-doored versions of open source software is the most obvious motive for such a stealthy and fairly sophisticated attack. SourceForge is in the process of validating updates to guard against potentially nasty surprises further down the line. It is also in the process of locking down servers and adding extra defences as a precaution against further attack.

The attack against SourceForge followed days after an attack on Fedora, another open-source outfit. Miscreants gained access through a team member's account, but there's no evidence that this compromised access was used to upload rogue code.

Two months ago the main source code repository of the Free Software Foundation was taken offline following an attack targeting website login credentials.