By: Dan Goodin, TheRegister.co.uk

The main source-code repository for the Free Software Foundation has been taken down following an attack that compromised some of the website's account passwords and may have gained unfettered administrative access.

The SQL-injection attacks on GNU Savannah exploited holes in Savane, the open-source software hosting application that was spun off from SourceForge, Matt Lee, a campaigns manager for the Free Software Foundation, told *The Register*. The attackers were then able to obtain the entire database of usernames and hashed passwords, some of which were decrypted using brute-force techniques.

Project managers took GNU Savannah offline on Saturday, more than 48 hours after the attack occurred. They expect to bring the site back online on Wednesday, although they're not guaranteeing it will be fully functional. Out of an abundance of caution, restored data will come from a backup made on November 24, prior to the compromise. Lee said there's no reason to believe any of the source code hosted on the site was affected by the breach.

“Version control systems that are in place for these projects actually would show a red flag in terms of any changes that they made, and we've not seen that, so we believe there's no issue there,” he explained. What's more, there's no indication that the FTP server used to actually transfer source code was compromised, he said.

The attackers used their access to add a hidden static HTML file to a CVS repository and a webpage that defaced the gnu.org home page. After finding a directory that was erroneously set to execute PHP scripts, the hackers also committed a PHP reverse shell script.

“They then proceeded to try a ton of root kits on the gnu.org webserver,” according to a time line provided by Lee. “We don't think they succeeded in getting root, but they may have.”

Project managers spent much of the weekend restoring the GNU website to its original state. Even after those steps were begun, the members discovered “that the cracking activity had resumed on www.gnu.org through PHP reverse shells running as user www-cvs,” the timeline said. “Realizing that the problem was much worse than we assumed at first, we immediately isolated the Savannah cluster and the GNU website from the network and start[ed] a deeper analysis.”

Managers said that all unsalted MD5 passwords stored on Savannah should be considered compromised and will have to be reset before the accounts can be re-enabled. The encrypted password scheme will also be upgraded to Crypt-MD5 (/etc/shadow's), and user password strength will be checked.

Lee said that Savane was already in the midst of an overhaul before the attack. It being open-source software that anyone can audit, one might have expected the SQL injection vulnerability to have been discovered and fixed long ago. To be fair, GNU.org is by no means the only popular open-source project to have been ransacked by hackers. Over the past 13 months, the heavily fortified website for the Apache Software Foundation has been breached twice