PHYS.ORG

osCommerce e-commerce software vulnerable to hackers, security researchers find

October 8 2013

(Phys.org) —A popular open-source software for e-commerce is vulnerable to being cheated, computer security researchers at the University of California, Davis, have found. By exploiting vulnerabilities in the widely used osCommerce software, the researchers were able to purchase items from online stores for free or substantially less than their correct prices.

"The majority of the payment modules in osCommerce are vulnerable to logic attacks that allow you to pay less or even pay nothing at all," said Fangqi Sun, a graduate student working with Professor Zhendong Su in the UC Davis Department of Computer Science.

The researchers have been attempting to notify osCommerce of the discovered vulnerabilities and to help the developers patch the software. They have also refunded the vendors for items they purchased at below cost during their research.

Online transactions rely on a trusted third party, or "cashier," who bridges the gap between vendors and their customers. But the use of a third party cashier also complicates the payment logic and introduces a new class of vulnerabilities that can result in significant financial losses to merchants, Su said.

The osCommerce software allows vendors to manage online transactions. It has been in active development and maintenance for about 12 years and is currently powering more than 14,000 online retailers. It is open-source software, meaning that programmers around the world can contribute and make improvements to it.

Sun, with Su and graduate student Liang Xu, downloaded the osCommerce software and developed the first automated tool to scan it for payment logic vulnerabilities.

Sun found for example, that with a few simple changes to HTTP requests she could pay for an item in U.S. dollars instead of the same amount of British pounds, a marked discount depending on the exchange rate. It was also possible to trick a merchant into believing that an item had been paid when in fact it had not.

The vulnerability detection tool was developed for the PHP programming language used to write osCommerce, but the general principles of the attacks should be applicable to other e-commerce software, whether proprietary or open-source, Sun said.

Earlier this year, Su's research group identified security flaws in popular applications running on Android smartphones.

Provided by UC Davis

Citation: osCommerce e-commerce software vulnerable to hackers, security researchers find (2013, October 8) retrieved 9 April 2024 from https://phys.org/news/2013-10-oscommerce-e-commerce-software-vulnerable-hackers.html