Security
May 5, 2009 4:07 PM PDT

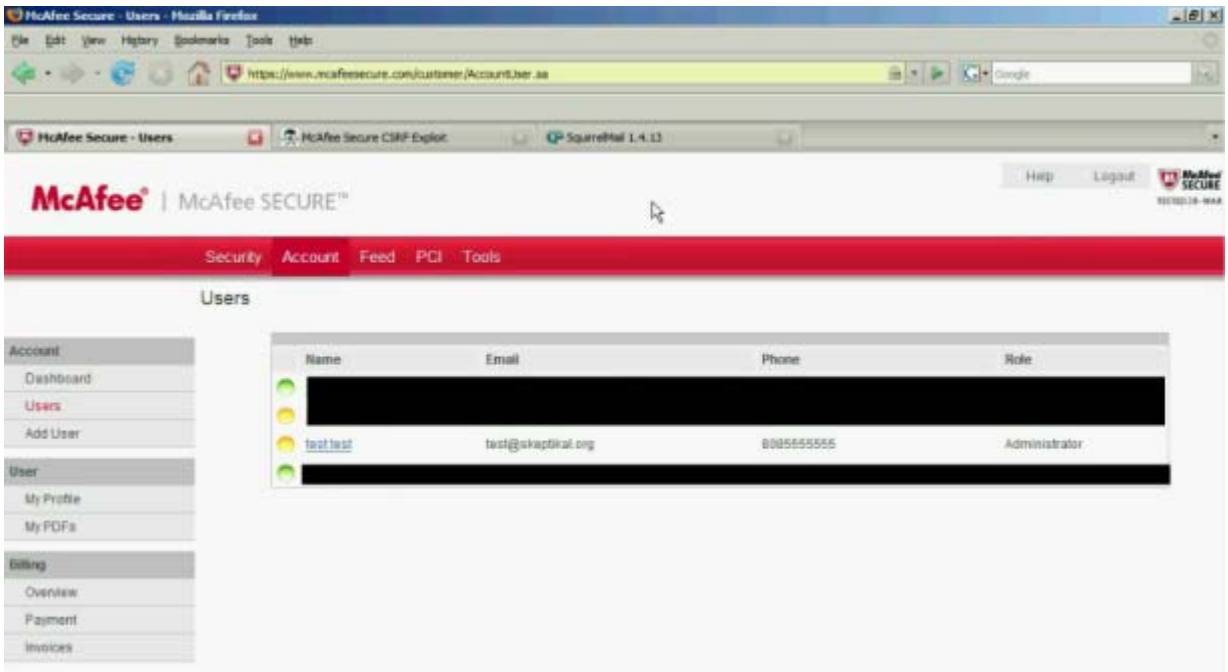
McAfee blasted for having holes in its Web sites

by Elinor Mills

Font size
Print
E-mail
Share

Yahoo! Buzz

Updated 5:15 p.m. PDT *with McAfee saying most of the vulnerabilities have been fixed.*



Security researcher Mike Bailey released this screen shot showing that he gained access to McAfee Secure via a cross-site request forgery hole.
(Credit: **Skeptikal.org**)

Security vulnerabilities on McAfee sites, including one designed to scan customers' sites for flaws, exposed certain customer accounts and could have been used for phishing attacks in which malware disguised as McAfee software could be distributed,

security experts say.

McAfee said late on Tuesday that most of the vulnerabilities were fixed, except for one part of the Web site that was taken offline to be fixed.

The McAfee sites were found to be vulnerable to cross-site scripting (XSS) attacks and cross-site request forgery attacks that could lead to phishing attacks on customers who think they are visiting the security vendor's site, according to **an article on ReadWriteWeb**.

Ironically, one of the vulnerable sites was McAfee Secure, which scans customer sites to determine if they are vulnerable to such attacks. The problem would signal that either McAfee doesn't run McAfee Secure across all of its own sites or the product doesn't work well, the report said.

To fall victim to a cross-site request forgery attack on that site, targets would have to be logged into their McAfee accounts and browse to a malicious Web site that exploits the vulnerability, according to the **Risky.biz** site.

Such attacks on sites of antivirus vendors are particularly dangerous because they enable attackers to create fake versions of security products that install Trojans or other malware and customers will trust it, Lance James, co-founder of Secure Science Corporation, told ReadWriteWeb.

The hole on the McAfee Secure site would indicate that the company failed to comply with PCI requirements for Approved Scanning Vendors, didn't use a secure software development lifecycle in building the application, and neglected to do an in-depth penetration test of the site, security researcher Mike Bailey wrote on his Skeptikal.org blog **on Monday**.

McAfee spokesman Joris Evers said the site taken offline was the McAfee Knowledge Center, which is part of its customer support site that uses software from a third-party provider. The site had a cross-site scripting vulnerability, he said.

"These types of vulnerabilities are rarely exploited in the wild and thus aren't deemed to be severe," he said in an e-mail. None of the vulnerabilities exposed any McAfee

corporate information and the company had not seen any malicious exploitation of the vulnerabilities, he added.

"McAfee has strict policies in place for its own Web sites and for services provided by third parties," Evers said. "We are investigating how these particular vulnerabilities were not identified in our screening process and will adjust our processes if necessary."

McAfee isn't the only security company to have security problems on its site. **Last month**, The Register reported on a cross-site scripting vulnerability on Symantec's site. And **in February**, a Romanian hacker site claimed to have used cross-site scripting and SQL injection attacks to breach the sites of F-Secure, Kaspersky, and BitDefender.

Elinor Mills covers Internet security and privacy. She joined CNET News in 2005 after working as a foreign correspondent for Reuters in Portugal and writing for The Industry Standard, the IDG News Service, and the Associated Press. E-mail Elinor.

Topics: **News**, **Vulnerabilities & attacks**

Tags: **McAfee**, **XSS**, **cross-site scripting**, **phishing**

Related

From CNET

McAfee launches free online cyber crime help center

Puerto Rico sites redirected in DNS attack

The Cold War moves to cyberspace

From around the web

Creating a Public Nuisance with Insecure... Washington Post Blogs - Securi...

Cybersecurity's Twitter-Fast Shifts Forbes.com