Sense of Security	Authorisation. Jason Edelstein
	Release date. 20 May 2011.

Sense of Security – Security Advisory – SOS-11-007.

PHPCaptcha / Securimage 2.0.2 – Authentication Bypass.

20 May 2011.

PHPCaptcha / Securimage 2.0.2 – Authentication Bypass - Security Advisory - SOS-11-007

Release Date.	20-May-2011
Last Update.	-
Vendor Notification Date.	04-Apr-2011
Product.	Securimage / PHPCaptcha
Platform.	PHP
Affected versions.	1.0.4 - 2.0.2
Severity Rating.	Medium
Impact.	Authentication bypass
Attack Vector.	Remote without authentication
Solution Status.	Vendor workaround (remove securimage_play.php)
CVE reference.	Not yet assigned

Details.

PHPCaptcha, also known as Securimage, is a popular Open Source PHP CAPTCHA library. It is also used in popular WordPress plugins such as the “Fast Secure Contact Form”.

Insufficient distortion in the audio version of the CAPTCHA allows an attacker to quickly decode the CAPTCHA by performing basic binary analysis of the generated audio file. The issue is compounded by the fact that even if the audio feature of the CAPTCHA has been disabled, it can still be accessed by forceful browsing to the /secure_play.php URI.

Proof of Concept.

Proof of concept code that works against the example_form.php page and the MP3 file format provided with the standard PHPCaptcha package available from www.phpcaptcha.org is available at:

http://www.senseofsecurity.com.au/advisories/SOS-11-007.zip

Proof of concept code is only available for the MP3 version of the audio, however the WAV audio format is also affected by the same vulnerability.

Solution.

Remove the script securimage_play.php and disable the use of the Audio CAPTCHA.

Discovered by.

Phil Taylor from Sense of Security Labs.

About us.

Sense of Security is a leading provider of information security and risk management solutions. Our team has expert skills in assessment and assurance, strategy and architecture, and deployment through to ongoing management. We are Australia's premier application penetration testing firm and trusted IT security advisor to many of the country's largest organisations.

Sense of Security Pty Ltd

Level 8, 66 King St
Sydney NSW 2000
AUSTRALIA

T: +61 (0)2 9290 4444
F: +61 (0)2 9290 4455
W: http://www.senseofsecurity.com.au
E: info@senseofsecurity.com.au
Twitter: ITsecurityAU

The latest version of this advisory can be found at:

http://www.senseofsecurity.com.au/advisories/SOS-11-007.pdf

Other Sense of Security advisories can be found at:

http://www.senseofsecurity.com.au/research/it-security-advisories.php