Sense of Security	Authorisation. Jason Edelstein
	Release date. 15 April 2011.

Sense of Security – Security Advisory – SOS-11-004.

cPassMan 1.82 – Arbitrary file download.

15 April 2011.

Sense of Security	Authorisation. Jason Edelstein
	Release date. 15 April 2011.

cPassMan 1.82 – Arbitrary file download – Security Advisory – SOS-11-004

Release Date.	15-Apr-2011
Last Update.	-
Vendor Notification Date.	7-Mar-2011
Product.	Collaborative Passwords Manager (cPassMan)
Platform.	Independent (PHP)
Affected versions.	1.82 (verified), and possibly others
Severity Rating.	Medium
Impact.	Local file system access
Attack Vector.	Remote without authentication
Solution Status.	Upgrade to v2.0, v1.x branch no longer updated
CVE reference.	Not yet assigned

Details.

A vulnerability has been discovered in the Collaborative Passwords Manager (cPassMan) web application that can be exploited to retrieve files from the local host file system.

The input passed to the component “sources/downloadfile.php” via the “path” variable allows the retrieval of any file on the local file system that the web server has access to. There is no data validation or authorisation mechanisms present within this component.

Proof of Concept.

http://localhost/cpassman/sources/downloadfile.php?path=C:\boot.ini

http://localhost/cpassman/sources/downloadfile.php?path=/etc/passwd

Solution.

The author (Nils Laumaillé) has indicated that the v1.x branch of cPassMan will no longer be updated, as he has rewritten the application and v2.0 is now the recommended release.

Discovered by.

Kaan Kivilcim 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-11-004.pdf

Other Sense of Security advisories can be found at:

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