

	Authorisation. <i>Jason Edelstein</i>
	Release date. 30 April 2009.

Sense of Security – Security Advisory – SOS-09-003.

Infor SCM SupplyWEB Multiple Vulnerabilities.

30 April 2009.

© Sense of Security 2009.	Editor Jason Edelstein.	Page No 1.
www.senseofsecurity.com.au	All rights reserved.	Version 1.0.



Authorisation.

Jason Edelstein

Release date.

30 April 2009.

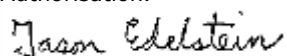
Infor SCM SupplyWEB Multiple Vulnerabilities - Security Advisory - SOS-09-003

Release Date.	30-Apr-2009
Last Update.	-
Vendor Notification Date.	23-Apr-2009
Product.	Infor SCM SupplyWEB
Platform.	Windows (verified), possibly others
Affected versions.	10.1.2 (verified), possibly others
Severity Rating.	Medium
Impact.	XSS issue: cookie/credential theft, impersonation, loss of confidentiality Authorisation issue: loss of confidentiality Local file inclusion: loss of confidentiality
Attack Vector.	XSS issue: remote by authenticated/unauthenticated user (depending on application component). Authorisation issue: remote without authentication. Local file inclusion issue: remote by authenticated user.
Solution Status.	Currently no solution
CVE reference.	CVE-2009-1793 CVE-2009-1795 CVE-2009-1794

Details.

Infor SCM SupplyWEB is a web-enabled Supplier Relationship Management solution. During an application penetration test Sense of Security identified multiple vulnerabilities within this application, including: Cross-site Scripting (XSS), insufficient access control, and Local File Inclusion problems.

© Sense of Security 2009.	Editor Jason Edelstein.	Page No 2.
www.senseofsecurity.com.au	All rights reserved.	Version 1.0.

	Authorisation. 
	Release date. 30 April 2009.

XSS issues:

The following application components (parameters) are vulnerable: textEditorPopUp.jsp (srcPage), listXRefParts (multiple), and viewFilterRelease (multiple). This occurred as a result of the application not properly filtering HTML tags which allowed malicious JavaScript to be embedded. When input is incorrectly validated and not properly sanitised and then displayed in a web page, attackers can trick users into viewing the web page and causing malicious code to be executed.

Insufficient access control issues:

The following application components display output to an unauthenticated user as they do not implement proper authorisation checks: listXRefParts and textEditorPopUp.jsp

Local File Inclusion issue:

The downloadBuyerFile application component is vulnerable to Local File Inclusion attacks. This allows an attacker to retrieve local files on a remote system which are accessible by the identity that the application server is launched with.

Proof of Concept.

XSS issue example:

```
http://IP_Address/supplyWeb/js/textEditorPopUp.jsp?srcPage="><script>var site =
"http://www.senseofsecurity.com.au";alert('XSS! Redirecting to ' %2B site %2B
'...');document.location.replace(site);</script>
```

Insufficient access control issue:

Retrieve listXRefParts and textEditorPopUp.jsp in your browser without first authenticating.

Local File Inclusion issue:

```
http://IP_Address/supplyWeb/gateway/downloadBuyerFile
POST variable: filename = ..\..\..\..\..\..\..\..\boot.ini
```

Solution.

The vendor has been advised of the issue, but has not yet issued a fix.

Discovered by.

Brett Gervasoni from SOS Labs.

© Sense of Security 2009.	Editor Jason Edelstein.	Page No 3.
www.senseofsecurity.com.au	All rights reserved.	Version 1.0.



Authorisation.

Jason Edelstein

Release date.
30 April 2009.

About us.

Sense of Security is a leading provider of IT 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 security consultancy and trusted IT security advisor to many of the countries largest organisations.

Sense of Security Pty Ltd

Level 3, 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

Advisory.

SOS-09-003 – <http://www.senseofsecurity.com.au/advisories/SOS-09-003.pdf>

© Sense of Security 2009.	Editor Jason Edelstein.	Page No 4.
www.senseofsecurity.com.au	All rights reserved.	Version 1.0.