FORTCONSULT

Straight talk on IT security

SECURITY ADVISORY

ID: FCSA1206

Site In A Box (SIAB) v 3.1

Cross Site Scripting (XSS) vulnerability

Phone: +45 70207525 Email: info@fortconsult.net Web: www.fortconsult.net

Background

SIAB is an ITERA product.

From the ITERA website (Google Translation):

"Itera Consulting was founded in 1999 and is today a leading Nordic company with more than 400 employees in offices in Denmark, Norway and Sweden. In addition, we have a development center in Ukraine, which gives us additional capacity and opportunities for cost-effective solutions for our customers.

We turnover of approx. DKK 400 million, is listed on the stock exchange in Oslo and our headquarters is located at Ullevaal Stadion in Oslo.

Our companies Itera Consulting Group complement each other. Our services ensure collaboration between business and IT. We challenge existing solutions and new thinking. We have customers of all sizes and with different challenges. We work with banks, insurance companies, telecommunications companies, energy supply industry and organizations - to name just a few examples.

Our employees are among the best in the industry. We follow constantly with the development that helps to create business value for our customers. We are passionate about our profession, are committed to our clients' business and does not compromise with the quality of our work.

With expertise in consulting, communications, user experience, SharePoint, portals, business intelligence, development,. Net, Java, project management, portfolio management, operation and SaaS, we are able to be the customer's IT advisor and partner in all aspects of the business, and thus total supplier.

Itera Consulting helps to create innovation, growth and a better future for our customers."

Description

Cross-Site Scripting attacks are a type of injection problem, in which malicious scripts are injected into the otherwise benign and trusted web sites. Cross-site scripting (XSS) attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user in the output it generates without validating or encoding it.

An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by your browser and used with that site. These scripts can even rewrite the content of the HTML page. (OWASP).

Phishing is the act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication.

Analysis

Attacker sends a malicious link and tricks victims into clicking it. Victims are more likely to click on it, since the link is to a valid site.

Attackers are usually execute scripts on victims to steal credentials as username and password.

Avoiding such flaws is extremely important as it's easy to execute and the effect is major.

Exploit

(tested on)

Version: SIAB 3.1

Malicious link for XSS:

http://www.example.com/admin/login.jsp?>'"><script>alert(31337)</script>

It is also possible to execute a phishing attack without executing scripts as:

Malicious link for Phishing:

http://www.example.com/admin/login.jsp?>'"<script><h1>This is a phishing attack, please call 555-hackers</h1>

CVE Reference

N/A at the release time.

Recommendations

1. Perform input validation.

Disclosure Timeline

27 November 2012 – Vulnerability found.

6 December 2012 – Vendor Notification – No reply from the vendor.

17 December 2012 – Vendor Notification (2nd try) – No reply from the vendor.

19 December 2012 – Public Disclosure.

The Security Research Team

This advisory has been discovered by FortConsult's Security Research Team/Yaniv Miron & Jan Skovgren.

About FortConsult

FortConsult provides independent security assessment services, including penetration testing and PCI DSS assessment service internationally to customers, such as financial services companies, banks, acquirers, service providers and merchants.

See www.fortconsult.com for more information about FortConsult.

Or contact us at +45 7020 7525 or info@fortconsult.net.

Copyright and Disclaimer