

[Full-disclosure] SiteStudio

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-05/0154.html>

From: Morning Wood (se_cur_ity_at_hotmail.com)

Date: 05/09/05

To: <full-disclosure@lists.grok.org.uk>

Date: Mon, 9 May 2005 05:57:25 -0700

– EXPL-A-2005-008 exploitlabs.com Advisory 037 –

– Site Studio –

AFFECTED PRODUCTS

=====

Site Studio

Positive Software Corporation

<https://www.psoft.net>

OVERVIEW

=====

SiteStudio is industry leading browser-based web site design and construction tool. It may also be fully and seamlessly integrated with H-Sphere. By using SiteStudio you add value to your Internet service by providing your customers with the easiest way to build a website. With SiteStudio, your users need not know anything about FTP, HTML, Telnet, HTTP, or imaging software. If they can surf the Internet, they can build their own professionally looking website.

note: Site Studio runs via Coyote/Jakarta on port 8080 by default

DETAILS

=====

1. persistent XSS in the guestbook

Site Studio guestbook does not filter HTML code from user-supplied input. A remote user can create a specially crafted entry that, when the page rendered, will cause arbitrary scripting to be executed by the user's browser. The code will originate from the site running the Site Studio software and will run in the security context of that site.

Full-Disclosure: [Full-disclosure] SiteStudio

Item 1

entering XSS type scripting in the name input field causes the script to be rendered upon visitation to the affected the page.

a.

Standalone Site Studio installations may be accessible on the target site via:

psoft.guestbook.GuestBookServ

[http://\[HOST\]:8080/studio/servlet/psoft.guestbook.GuestBookServ](http://[HOST]:8080/studio/servlet/psoft.guestbook.GuestBookServ)

b.

Integrated Site Studio with H-Sphere may be accessible on the target site via:

E-Guest_sign.pl

[http://\[host\]/cp/Scripts/perl/guestbook/E-Guest_sign.pl](http://[host]/cp/Scripts/perl/guestbook/E-Guest_sign.pl)

SOLUTION:

=====

Psoft has been contacted and patches released:

item a:

http://www.psoft.net/SS/ss_16_security_update_guestbook.html

item b:

http://www.psoft.net/misc/hsphere_winbox_security_update_guestbook.html

Credits

=====

This vulnerability was discovered and researched by
Donnie Werner of exploitlabs

Donnie Werner

mail: wood at exploitlabs.com

mail: morning_wood at zone-h.org

--

web: <http://exploitlabs.com>

web: <http://zone-h.org>

<http://exploitlabs.com/files/advisories/EXPL-A-2005-008-sitestudio.txt>

Full-Disclosure - We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia - <http://secunia.com/>