LIONIC®
Security Chip Provider

03/05/2011
Doc No: SN-2011-18003

Security News
2011-18003 vtiger CRM 5.2.1 Cross-Site Scripting Vulnerability

1. Affected Version

vtiger CRM version 5.2.1

2. Description

1. vtiger CRM is a free, full-featured, 100% Open Source CRM software ideal for small and medium businesses, with low-cost product support available to production users that need reliable support.

2. There is a reflected cross-site scripting vulnerability found in vtiger CRM version 5.2.1 can be exploited to execute arbitrary JavaScript.

3. Vulnerability Analysis

The proof-of-concept code is listed as follows:

```
http://localhost/vtigercrm/vtigerservice.php?service=%3Cscript%3Eal-
ert%280%29%3C/script%3E
```

Table 1: The proof-of-concept code

This flaw is caused due to improper validation of user-supplied input by the vtigerservice.php script. This may allow an attacker to create a specially crafted URL that would execute arbitrary script code in a victim's browser and even steal the victim's cookie-based authentication credentials.

4. Recommendation

1. Lionic IDP signature database can prevent this attack since 03/05/2011.
2. Upgrade to the latest non-affected version of the software.

5. Reference

1. http://packetstormsecurity.org/files/view/100183/vtigerCRM5.2.1-XSS.txt

About Lionic: Lionic Corporation is an innovative network security chip and IP design company. It provides optimal cost-performance solutions for network security products from 30Mbps SOHO devices to 4Gbps enterprise-level appliances.
For more information, please visit Lionic website and contact our sales representatives.
Web site: www.lionic.com e-mail: sales@lionic.com Tel: 886-3-578-9399 Fax: 886-3-578-0707