security-assessment.com

Vulnerability Advisory

Name	SugarCRM – Local File Disclosure
SugarCRM Advisories	http://www.sugarcrm.com/docs/Release_Notes/OpenSource_ReleaseNotes_4.5.1j/Sugar_Release_Notes_4.5.1j.2.6.html (Bug 20522) http://dl.sugarforge.org/sugarcrm/SugarCE5.0Latest/SugarCE5.0.0/Sugar_CommunityEdition_ReleaseNotes_5.0c.pdf (Bug 20342)
Date Released	4.5.1j in March 24, 2008 and 5.0.0c in April 4, 2008
Affected Software	SugarCRM - Community Edition Version 5.0.0 SugarCRM – Community Edition Version 4.5.1
Researcher	Roberto Suggi Liverani roberto.suggi@security-assessment.com

Description

SugarCRM Community Edition is vulnerable to local file contents disclosure. This vulnerability can be exploited by a malicious user to disclose potentially sensitive information. The flaw is caused due to a lack of input filtering in the SugarCRM RSS module, which can be exploited to disclose the content of local files.

The RSS module allows SugarCRM users to add RSS feeds to their personal RSS list. The application expects an URL value pointing to a valid RSS feed. However, the URL variable value is not properly sanitised and any URI value can be entered instead. In this particular case, it was discovered that it is possible to enter a file path to any files on the local system hosting the SugarCRM application.

As a result SugarCRM does not display the new RSS feed in the list as it is not a valid RSS URL Feed. However, the application creates a local file with the filename of the md5 hash of the URL entered. The file is created in the directory cache/feeds . If the Apache web server is used, the file is created with the user www-data containing read permission.

Exploitation

An exploitation example in a LAMP (Linux, Apache, Mysql, PHP) environment:

If an authenticated attacker enters a value of "/etc/passwd" (without quotes) in the RSS URL field, the application will generate a MD5 hash of the string containing the file path. In this case, the value "/etc/passwd" is hashed to "c5068b7c2b1707f8939b283a2758a691" (without quotes). The MD5 hash is then used as a filename with the file contents of /etc/passwd. The file /etc/passwd can then be viewable publicly at http://sugarwebsiteaddress/cache/feeds/c5068b7c2b1707f8939b283a2758a691 .
Exploitation of this flaw does not require authentication.

The URL variable is handled by the /modules/Feeds/Feed.php page. The array variable $url is passed without filtering to the xml_domit_rss_document function at the following line:

$rssdoc = new xml_domit_rss_document ($this->url, 'cache/feeds/', 3600);

The XML domit RSS plugin is then called and retrieves the file content at the path given and then generate the MD5 hashed file in the cache/feeds folder as instructed by the function in Feed.php .

Solution

Install the vendor supplied patches.
Patch 4.5.1j: http://www.sugarcrm.com/forums/showthread.php?t=31688
Patch 5.0.0c: http://www.sugarcrm.com/forums/showthread.php?t=32252

About Security-Assessment.com

Security-Assessment.com is Australasia's leading team of Information Security consultants specialising in providing high quality Information Security services to clients throughout the Asia Pacific region. Our clients include some of the largest globally recognised companies in areas such as finance, telecommunications, broadcasting, legal and government. Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients.

Security-Assessment.com is committed to security research and development, and its team continues to identify and responsibly publish vulnerabilities in public and private software vendor's products. Members of the Security-Assessment.com R&D team are globally recognised through their release of whitepapers and presentations related to new security research.

For further information on this issue or any of our service offerings, contact us

Web www.security-assessment.com
Email info@security-assessment.com
Phone +649 302 5093