Security Research Advisory

Hummingbird Collaboration
Multiple Vulnerabilities

Table of Contents

Summary

Hummingbird Collaboration is a Web-based collaborative groupware for teams across and beyond the enterprise. It integrates different works on single projects accessed by several concurrent users, improving efficiency, organization and automated workflow.

Regular and registered users can easily access to all project information, documents, discussion threads, tasks list through the Web.

It includes several utilities like messaging system, project & file manager and a Web calendar.

Date	Details
20/12/2005	Vendor disclosure
21/12/2005	Vendor acknowledgment
-	Patch release
10/01/2006	Public disclosure

Stored Cross-Site Scripting

<table>
<tr><td colspan="5">Stored Cross-Site Scripting</td><td>Advisory Number</td></tr>
<tr><td colspan="5"></td><td>SN-06-01</td></tr>
<tr><td>Severity</td><td>Software</td><td>Version</td><td>Accessibility</td><td>CVE</td><td>Author(s)</td></tr>
<tr><td rowspan="3">M</td><td>Hummingbird Collaboration</td><td>≤ 5.2.1</td><td>Remote</td><td>n/a</td><td rowspan="3">Luca Carettoni
Federico Maggi</td></tr>
<tr><td colspan="2">Vendor URL</td><td colspan="2">Advisory URL</td></tr>
<tr><td colspan="2">-</td><td colspan="2">-</td></tr>
</table>

Vulnerability Details

A second-order XSS have been found. It allows permanent scripting by uploading malicious client side scripts by embedding them in a HTML page. Hummingbird Collaboration does not verify the content of HTML files during the uploading process. In addition, the collaborative groupware does not force the HTML to be downloaded (e.g. forcing the "Content-Disposition" property): As a result, the HTML page and embedded scripts are normally interpreted and rendered by the user browser.

An attacker could (1) plan session hijacking attacks, (2) prepare phishing (a regular user could be tricked by presenting him/her with a fake login page) and (3) affect the usability and the availability of the service.

Technical Details

Description

An attacker can simply upload an HTML file with embedded malicious scripts (e.g. Javascript) using the file manager utility.

Improper File Handling

Improper File Handling					Advisory Number
					SN-06-01
Severity	Software	Version	Accessibility	CVE	Author(s)
L	Hummingbird Collaboration	≤ 5.2.1	Remote	*n/a*	Luca Carettoni Federico Maggi
	Vendor URL		Advisory URL		
	-		-		

Vulnerability Details

Using a crafted URL, a user could force the download of a previously uploaded file changing its original name. By exploiting this vulnerability, a regular user can be tricked about file content and filename of what he/she's downloading.

Technical Details

Description

An attacker would need to trick the user into downloading a certain file with a crafted URL, like the following one.

PoC URL:

```
https://mySite/hc/hc/fake.doc?d=fc&o=dwnd&fid=1189762&did=89777&x=16080&doc_ext=.txt
```

In this example, the file with id equal to 1189762 is downloaded, changing the name and the type of txt file in "fake.doc". Other techniques (e.g. XSS) make it easy to create a fake link similar to the previous one.

Information Disclosure

Information Disclosure					Advisory Number
					SN-06-01
Severity	Software	Version	Accessibility	CVE	Author(s)
L	Hummingbird Collaboration	≤ 5.2.1	Remote	*n/a*	Luca Carettoni Federico Maggi
	Vendor URL		Advisory URL		
	-		-		

Vulnerability Details

By inspecting some application responses it is possible to get more information about the parameters type and format. Instead of displaying generic error messages, detailed information are sent to the client (e.g. the parameter must be TRUE or FALSE). Moreover, by inspecting the application cookies is it possible to get internal network information about the IP address of the application server.

Technical Details

Description

In most cases it just involves the inspection of server responses. The following URL shows an example of improper error handling.

PoC URL:

```
https://mySite/hc/hc?d=mes&x=20433&ntb=[numericParam]
```

Using [numericParam] instead of a string parameter.

The internal IP address is "encoded" into the cookie name (e.g. *com.peopledoc.rhum.JURA_SESSION_ID_192.168.1.1_0.71221182=972323;*).

Legal Notices

Secure Network (*www.securenetwork.it*) is an information security company, which provides consulting and training services, and engages in security research and development.

We are committed to open, full disclosure of vulnerabilities, cooperating with software developers for properly handling disclosure issues.

The information in the advisory is believed to be accurate at the time of publishing based on currently available information. This information is provided as-is, as a free service to the community by Secure Network research staff. There are no warranties with regard to this information. Secure Network does not accept any liability for any direct, indirect, or consequential loss or damage arising from use of, or reliance on, this information.

If you have any comments or inquiries, or any issue with what is reported in this advisory, please inform us as soon as possible.

e-mail	info@securenetwork.it
phone	+39 02 917 730 41