SAP'S BACKDOOR

Dmitry Gutsko
blog.ptsecurity.com/2013/08/saps-backdoor.html

SAP security analysis is one of my basic duties at Positive Technologies. Besides, I needed a topic to speak about at PHDays III forum. Finally, I decided on the following: how to hide a user with the SAP_ALL profile (i.e. all possible authorizations) in the SAP system. If a malicious user manages to log on the system and gets authorized to create users and assign privileges to them, then he/she will probably try to create their own account, certainly with all authorizations in the system. However, internal checks and external audits list such users; thus, there is no chance for a user with SAP_ALL permissions to go unnoticed.

Well, let's start. I've set two vectors for my research:

1. Cheat authorization analysis reports using nested profiles, reference users, roles, profile copies, etc.
2. If you ask SAP specialists how to list users with particular authorizations, they will advise to try transaction SUIM and Report RSUSR002, which is almost the same. Based on the analysis of ABAP code from Report RSUSR002, create a mechanism to bypass the report algorithm and hide the user.

If you are interested in the first vector, you are welcome to have a look at my presentation [1]; the second one is detailed below.

Let's turn now to the logic in the report. It is simple: you take the list of all user accounts and check each user for the given authorizations. If a user does not comply with the search criteria, it is removed from the list. It seems easy... but the following string attracts our attention during analysis:

A user with such a mysterious name '.....' (12 dots) is removed from the list. Let's test our assumption. We will create a user with the name of 12 dots, assign it with different roles and profiles, and then check the report results. As expected, there is no such username in the results!

Isn't it interesting, why SAP implemented such a thing? I cannot answer this question for sure. This user might be created while generating EARLYWATCH reports and might serve some particular purpose in the system.

The vulnerability was assigned with the following CVSS vector:

```
CVSS Base Score: 4.6
CVSS Base Vector: AV:N/AC:H/
AU:S/C:P/I:P/A:P
```

The severity level is not high of course. However, you will likely feel distressed to know that the vendor of the system, where you store and process all your critical business data, has left such a back door to conceal some specifically crafted users. What was the real purpose of that?

The situation is not that bad though. The patch for this vulnerability was released in June 2013 (see SAP Note 1844202). With the security update installed, you will rid your systems of such problems.

According to the table below, the patch was created for all SAP_BASIS versions starting from 46B. In other words, if you have not updated your system yet, then this vulnerability is ensured in your system.

Reference list:
1. http://www.slideshare.net/slideshow/embed_code/22591696
2. SAP Security note 1844202: https://service.sap.com/sap/support/notes/1844202

```
1502
1503            lv_start = lv_end + 1 .
1504            IF lv_start > lv_lin_cnt .
1505              EXIT .
1506            ENDIF.
1507          ENDDO.
1508        ENDTRY.
1509        DELETE userlist WHERE bname = '..........'.
1510      ENDIF.
```

Affected Releases

Software Component	Release	From Release	To Release
SAP_BASIS	46	46B	46D
SAP_BASIS	60	620	640
SAP_BASIS	70	700	702
SAP_BASIS	71	710	730
SAP_BASIS	731	731	731
SAP_BASIS	740	740	740