

# [UNIX] SAP Database Local Root Vulnerability During the Installation Process

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-04/0060.html>

---

*support\_at\_securiteam.com*

*Date:* 04/27/03

To: list@securiteam.com

Date: 27 Apr 2003 21:43:59 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

In the US?

Contact Beyond Security at our new California office housewarming rates on automated network vulnerability scanning. We also welcome ISPs and other resellers!

Please contact us at: 323-882-8286 or [ussales@beyondsecurity.com](mailto:ussales@beyondsecurity.com)

-----

SAP Database Local Root Vulnerability During the Installation Process

---

## SUMMARY

<<http://www.sapdb.org>> SAP DB is a Free Enterprise database. An exploitable race condition exists during installation that can be won to yield root to a local malicious user. An executable is world writeable before a setuid bit is set by the installation program.

## DETAILS

Vulnerable systems:

- \* SAP DB version 7.3.0.29
- \* SAP DB version 7.4.3.7 beta

Installation of the SAP database is done by the binary SDBINST. This first decompresses the files, changes permissions and then runs a file integrity check. Once this check is completed setuid bits are added to two files. A large gap between this check and the setuid operation exists (a few seconds at i least). This gives us ample time to change the contents of the pre-setuid file.

## Securiteam: [UNIX] SAP Database Local Root Vulnerability During the Installation Process

For the production 7.3.0.29 version:

Before the setuid root bit is set, a log file is written to that a normal non-privileged user can read. This file was located in /tmp/sapdb-server-linux-32bit-i386-7\_3\_0\_29/y/config/install/. We simply watch that file for what is written to it just before the call to chmod and copy our malicious code over the target binary.

Below is a partial analysis of SDBINST.

```
chmod("/usr/sapdb/depend/pgm/lserver", 0100777) = 0
```

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

### DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.