

[UNIX] SuSE sdbsearch.cgi Security Weakness

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-08/0027.html>

From: support@securiteam.com

Date: 08/02/01

From: support@securiteam.com

To: list@securiteam.com

Subject: [UNIX] SuSE sdbsearch.cgi Security Weakness

Message-Id: <20010802194209.954A713902@mail.der-keiler.de>

Date: Thu, 2 Aug 2001 21:42:09 +0200 (CEST)

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

SuSE sdbsearch.cgi Security Weakness

SUMMARY

The sdbsearch.cgi script is a part of SuSE distribution. A vulnerability in this script allows attackers that are able to write local files (even unprivileged local files) to get them executed with the privileges that sdbsearch.cgi runs with.

DETAILS

Affected systems:

SuSE version 6.x

SuSE version 7.x (7.1 and 7.2 have tainting protection, but even with it is still possible to pass sdbsearch files that should not be read)

Sdbsearch.cgi trusts the content of HTTP_REFERER variable, a variable that is set by client during HTTP requests. Pieces of this data (the HTTP_REFERER) are used later in the search engine (as keywords or referring files).

A vulnerability in the script occurs if there is the possible of writing local files on the target host (e.g. uploading through FTPd or any other method). A vulnerability in the program allows attackers that access this file to cause the sdbsearch to execute the arbitrary commands. This is caused because sdbsearch will use the open() function to open up the "keylist.txt" file which is known to be vulnerable to the standard pipe open() based attack (only this time without the -T option).

Hypermail Development List: [UNIX] SuSE sdbsearch.cgi Security

Exploit:

Proof of concept is very simple; just create a harmful keylist.txt in /tmp directory and send a request to HTTP that looks like this:

```
GET /cgi-bin/sdbsearch.cgi?stichwort=keyword HTTP/1.0
Referer: http://example.org/../../../../tmp
```

```
/tmp/keylist.txt can include something of the sort of:
$ echo -e "keyword\0touch exploitable|" > /tmp/keylist.txt
```

After a successful attempt, there will be "exploitable" file in /tmp directory.

Patch:

Filter the HTTP_REFERER variable.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:z33d@eth-security.net>>
Maurycy Prodeus.

=====

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.

-
- *Next message:* support@securiteam.com: "[UNIX] KRB5 TelnetD Buffer Overflows"
 - *Previous message:* support@securiteam.com: "[EXPL] Quake 3 Arena Security Vulnerability (CHAR 255, Exploit)"
 - *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)