

[UNIX] Sun AnswerBook2 Gettransbitmap Buffer Overflow Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-05/0084.html>

From: support@securiteam.com

Date: 05/21/02

From: support@securiteam.com

To: list@securiteam.com

Date: Tue, 21 May 2002 08:39:44 +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>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> – Know that you're safe.

Sun AnswerBook2 Gettransbitmap Buffer Overflow Vulnerability

SUMMARY

Sun <<http://www.sun.com/software/ab2/>> AnswerBook2 is vulnerable to a stack based buffer overflow condition that can allow a remote attacker to execute arbitrary code. The problem is due to the gettransbitmap CGI that comes with AnswerBook2 not correctly performing bounds checking on the filename argument. A remote attacker can create a request that will result in arbitrary code execution with user daemon privileges.

DETAILS

Vulnerable systems:

* Sun AnswerBook2 versions 1.4, 1.4.1, 1.4.2, 1.4.3

Technical Recommendation:

Presently, there are no vendor patches available. As a workaround solution, remove access to the gettransbitmap binary.

```
#chmod 0000 <path to>/gettransbitmap
```

Otherwise, disable AnswerBook2.

Securiteam: [UNIX] Sun AnswerBook2 Gettransbitmap Buffer Overflow Vulnerability

Vendor Status:
Vendor notified.

ADDITIONAL INFORMATION

The information has been provided by
<mailto:researchteam@esecurityonline.com> Kevin Kotas.

=====

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.

-
- **Previous message:** support@securiteam.com: "[NEWS] Xitami CGI Processing Failure Vulnerability"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)