

[UNIX] Snif File Disclosure Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-12/0004.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 12/01/03

To: list@securiteam.com

Date: 1 Dec 2003 13:46:48 +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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Snif File Disclosure Vulnerability

SUMMARY

<<http://www.bitfolge.de/index.php?l=en&s=snif&style=earth>> Snif is "a simple and nice index file". A vulnerability in the product allows remote attackers to download files that reside outside the bound HTML root directory.

DETAILS

Vulnerable systems:

- * Snif versions prior to 1.2.5

Immune systems:

- * Snif version 1.2.5

The script takes two query-strings "path" and "download" from the URL and concatenates them. It stores the result in the variable \$filename which is the file to be downloaded. By default the value for the path variable is set to NULL and there is no error checking to see if the "download" querystring is outside the default directory. Thus an attacker could change the "download" querystring to any file on the file system while leaving the "path" NULL. This would allow him/her to download the file requested.

Securiteam: [UNIX] Snif File Disclosure Vulnerability

Vulnerable code:

```
// this handles the download requests
if ($_GET["download"]!="") {
  // This is were the path checking fails
  $filename = $path.$_GET["download"];
  if (
    !file_exists($filename)
    OR fileIsHidden($_GET["download"])
    OR (substr(strtolower($_GET["download"]), -4)==".php" AND
    !$allowPHPDownloads)) {

    Header("HTTP/1.0 404 Not Found");
    echo "<b>Error: File not found.</b><br><br>we suggest you
    <a href=\"".$_SERVER["HTTP_REFERER"]."\">go back</a>";
  } else {
    Header("Content-Length: ".filesize($filename));
    Header("Content-Type: application/x-download");
    Header("Content-Disposition: attachment;
filename=\"".$_GET["download"]");
    readfile($filename);
  }
  die();
}
```

Exploit:

By requesting the following URL

<http://www.yourserver.com/snif/index.php?download=/etc/passwd>, it is possible to download the /etc/passwd file.

Solution:

Download version 1.2.5 from the vendors homepage

<<http://www.bitfolge.de/snif>> <http://www.bitfolge.de/snif>.

Vendor timeline:

24 November 2003 – Bug Found

25 November 2003 – Vendor Contacted

26 November 2003 – Vendor Fixed Bug

ADDITIONAL INFORMATION

The information has been provided by <mailto:jay@j-security.co.uk> J.

=====

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

=====

=====

Securiteam: [UNIX] Snif File Disclosure Vulnerability

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.