

[NEWS] mnoGoSearch Found To Be Vulnerable to a Heap Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-05/0051.html>

From: support@securiteam.com

Date: 05/11/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sat, 11 May 2002 23:18:21 +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.

mnoGoSearch Found To Be Vulnerable to a Heap Overflow

SUMMARY

<<http://www.mnogosearch.org/>> mnoGoSearch is a full-featured SQL based web search engine, a vulnerability in the product allows attackers to cause the product to overflow one of its internal heap buffers, causing the program to crash, possibly execute arbitrary code.

DETAILS

Vulnerable systems:

mnoGoSearch version 3.1.9 and prior

Immune systems:

mnoGoSearch version 3.2.0

Whenever mnoGoSearch receives a too long query string (q var), search.cgi segfaults (Example: <http://127.0.0.1/cgi-bin/search.cgi?q=query>). The bug resides in a bad management of heap-allocated memory. The bug could be abused by remote attackers to execute code with web server privileges.

Solution:

Authors were contacted a month ago: they told notified that the CVS

Securiteam: [NEWS] mnoGoSearch Found To Be Vulnerable to a Heap Overflow

version had been fixed. Currently you should disable search.cgi, or alternatively use the patch attached to this advisory (for 3.1.19) or install last CVS version.

Patch:

```
--- src/search.c Tue Jun 26 10:55:17 2001
+++ src/search.c Wed May 8 15:17:12 2002
@@ -1403,6 +1403,13 @@
     */
     if(!UDM_STRNCMP(token,"q=")){
         char str[UDMSTRSIZ]="";
+ /* Really temporary security fix */
+ if(strlen(token) > 512)
+ {
+ printf("<html><body>Query string too long</body></html>\n");
+ exit(1);
+ }
+ /* q1--- */
         query_words=strdup(UdmUnescapeCGIQuery(str,token+2));
         query_url_escaped=strdup(UdmEscapeURL(str,query_words));
         query_form_escaped=UdmHtmlSpecialChars(query_words);
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:qitest1@bespin.org> qitest1.

=====

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: "[NT] NTFS and PGP Interact to Expose EFS Encrypted Data"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)