

# [NT] SMSGate Denial of Service

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-03/msg00003.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxx)>
  - *Date:* 3 Mar 2008 16:32:49 +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>

-----

SMSGate Denial of Service

---

## SUMMARY

<<http://www.netwinsite.com/smsgate/>> SMSGate is "a gateway from Email to SMS and back". A vulnerability in the way SMSGate handles incoming HTTP requests allows remote attackers to cause the server to crash.

## DETAILS

Vulnerable Systems:

- \* SMSGate version 1.1n

SMSGate provides both the SMTP/SMS interface and a SSL web administration service running on port 8775 and by default accessible only locally (127.0.0.1).

When a too big HTTP Content-Length value is received, the server tries to allocate the specified amount of memory and when fails shows a debug messagebox in which the admin must choose if aborting the application, debugging it or ignoring the problem (in which case the server will continue to work correctly).

The entire server will be completely unreachable for all the time the

## [NT] SMSGate Denial of Service

Ignore button is not selected, so nobody can send SMS and the remote admin can't manage the server.

Exists also another problem caused by a malformed or non-existent Content-Length value which causes only the showing of an error message box (about the impossibility of writing the NULL delimiter at uninitialized pointer at offset 0xcccccccc) since the server will continue to work correctly.

Note the limitation described at the beginning of this section (local IPs only) doesn't affect the exploiting of the vulnerability, so any attacker from any IP address can block the server.

Exploit:

Send the following HTTP request through netcat + stunnel:

```
POST / HTTP/1.0
Content-Length: -1
```

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:aluiigi@xxxxxxxxxxxxxxx>> Luigi Auriemma.

The original article can be found at:

<<http://aluiigi.altervista.org/adv/smsgheit-adv.txt>>  
<http://aluiigi.altervista.org/adv/smsgheit-adv.txt>

=====

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.