

# [UNIX] Squid Analysis Report Generator Buffer Overflow

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-03/msg00005.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 3 Mar 2008 18:46:08 +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>

-----

Squid Analysis Report Generator Buffer Overflow

---

## SUMMARY

<<http://sarg.sourceforge.net>> Squid Analysis Report Generator is "a tool that allow you to view "where" your users are going to on the Internet". Execution of arbitrary code in Squid Analysis Report Generator is possible by executing sarg with specially crafted squid log files (access and useragent log).

## DETAILS

Vulnerable Systems:

- \* Squid Analysis Report Generator version 2.2.3.1

Immune Systems:

- \* Squid Analysis Report Generator version 2.2.4

The access.log has to be manually created to trigger the exploit, as Squid will not allow malformed HTTP methods.

The useragent log is more critical, as this vulnerability can be exploited by just passing the useragent string within a request to the Squid proxy.

## [UNIX] Squid Analysis Report Generator Buffer Overflow

### PoC/Exploit:

Edit a normal access log and set the request method to an overly long string.

Edit a normal useragent log and set the useragent field to an overly long string or send a request to the Squid proxy server passing an overly long string as useragent in the HTTP header.

### Disclosure Timeline:

2008-01-28 – vendor informed  
2008-01-28 – vendor responded  
2008-03-02 – vendor released new version  
2008-03-03 – public disclosure

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:l4teral@xxxxxxxxxx>> L4teral.

=====

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@xxxxxxxxxxxxxxxx](mailto:list-unsubscribe@xxxxxxxxxxxxxxxx)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@xxxxxxxxxxxxxxxx](mailto:list-subscribe@xxxxxxxxxxxxxxxx)

=====

=====

### 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.