

[NEWS] Blogger.com HTTP Response Splitting Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-01/msg00075.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 19 Jan 2006 16:47:26 +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>

Blogger.com HTTP Response Splitting Vulnerability

SUMMARY

" <<http://www.blogger.com/>> Blogger.com is a blogging system of Google." Blogger has been found to not filtering characters that can affect the HTTP headers response, this causes the portal to become vulnerable to HTTP response splitting XSS.

DETAILS

Blogger's personal page redirection mechanism contains a classic HTTP response splitting vulnerability in the "Location" HTTP header. The problem occurs due to use of unsensitized user-supplied data in the "Location" HTTP header, which enables attacker to inject CRLF(%0d%0a) characters thus splitting server's response taking full control over the contents of second HTTP response. Exploitation of the vulnerability can lead to cross-site scripting (XSS), cache poisoning and phishing attacks.

Proof of Concept:
[http://www.blogger.com/r?\[URL here\]](http://www.blogger.com/r?[URL here])

Disclosure Timeline:

[NEWS] Blogger.com HTTP Response Splitting Vulnerability

02/01/2006 – Issue discovered. Vendor notified.
02/01/2006 – Initial vendor response.
12/01/2006 – Vendor inquired on status.
13/01/2006 – Vendor response and confirmation that bug fixed.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:meder@xxxxxx>> Meder Kydyraliev.

The original article can be found at:

<http://o0o.nu/~meder/o0o_Blogger_HTTP_response_splitting.txt>

http://o0o.nu/~meder/o0o_Blogger_HTTP_response_splitting.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@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: 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.



- Prev by Date: [*\[NEWS\] Cisco Call Manager Privilege Escalation*](#)
- Next by Date: [*\[NEWS\] Oracle Database and Report Engine Multiple Vulnerabilities*](#)
- Previous by thread: [*\[NEWS\] Cisco Call Manager Privilege Escalation*](#)
- Next by thread: [*\[NEWS\] Oracle Database and Report Engine Multiple Vulnerabilities*](#)
- Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)