

# [NT] Cross-Site Scripting Vulnerability in Wrensoft Zoom Search Engine

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-10/0063.html>

---

*From:* SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

*Date:* 10/15/03

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 15 Oct 2003 10:22:11 +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>

-----

Cross-Site Scripting Vulnerability in Wrensoft Zoom Search Engine

---

## SUMMARY

<<http://www.wrensoft.com/zoom/>> Zoom is "the easiest and most straight forward way to add a powerful custom search engine to your website". A vulnerability in the product allows remote attackers to cause to product to return arbitrary HTML and/or JavaScript.

## DETAILS

Vulnerable systems:

\* Zoom version 2.0 – Build: 1018

The Zoom Search engine does not properly filter user-supplied input when displaying the search results. This issue allows remote attacker to inject malicious code in the target system. All the code will be executed within the context of the website. An example of such an attack is

[http://www.victim.com/search.php?zoom\\_query=<script>alert\("hello"\)</script><script>alert\("hello"\)</script>](http://www.victim.com/search.php?zoom_query=<script>alert(\)

In order for the attack to work, a user must click on one of these specially crafted URLs, which can be sent by email to the user, or by the

Securiteam: [NT] Cross-Site Scripting Vulnerability in Wrensoft Zoom Search Engine

using clicking on a link.

Impact:

It is possible for an attacker to retrieve information from a user's system.

Solution:

Upgrade to Build 1019. This can be downloaded from  
<<http://www.wrensoft.com/ftp/zoomsearch.exe>>  
<http://www.wrensoft.com/ftp/zoomsearch.exe>.

Vulnerability History:

- 30 Sep 2003 Identified by Ezhilan of Sintelli
- 01 Oct 2003 Issue disclosed to Wrensoft
- 02 Oct 2003 Second notification to Wrensoft
- 02 Oct 2003 Vulnerability confirmed by Raymond Leung of Wrensoft.
- 08 Oct 2003 Sintelli informed of fix Wrensoft
- 08 Oct 2003 Sintelli confirms vulnerability has been addressed
- 08 Oct 2003 Build 1019 available
- 09 Oct 2003 Sintelli Public Disclosure

ADDITIONAL INFORMATION

The information has been provided by Ezhilan of  
<<mailto:sintraq@sintelli.com>> Sintelli SINTRAQ.

=====

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

=====  
=====

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.