

[UNIX] The Everything Development System SQL Injection

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-02/msg00002.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 3 Feb 2008 09:05:13 +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>

The Everything Development System SQL Injection

SUMMARY

There exists a vulnerability in The Everything Development Engine that allows a user to inject their own SQL to modify a SELECT query, leading to information disclosure, XSS, or privilege escalation. What's more, passwords are stored in the database as plaintext, making user accounts very easily compromised.

DETAILS

Vulnerable Systems:

- * The Everything Development System version Pre-1.0 and prior

In some versions of the software sub has encountered, the following proof of concept will display a corresponding username and password in the "core" field and "reputation" field on the page, respectively.

Proof of Concept:

[http://path.to/cms/index.pl?node_id=0/**/UNION/**/SELECT/**/null,101,null,1,null,null,passwd,null,null,nick,null/**/FROM/**/user/**/WHERE/**/nick/**/!%3d/**/"/**/%23](http://path.to/cms/index.pl?node_id=0/**/UNION/**/SELECT/**/null,101,null,1,null,null,passwd,null,null,nick,null/**/FROM/**/user/**/WHERE/**/nick/**/!%3d/**/)

In other, probably more recent versions, a 13-column query is required or the UNION. What does not change, is that of all of the various versions I've encountered, all are vulnerable to SQL injection.

The ideal fix would be to ensure that the 'node_id' request variable is the appropriate data-type (signed int) before passing it as part of a SQL query.

Vendor Status:

A private ticket was created on the vendors Bug Tracker page prior to this release. However, sub has decided to release this vulnerability without a reply from the vendor as the Bug Tracker, and development project, seemed to be 'abandoned.'

ADDITIONAL INFORMATION

The information has been provided by <<mailto:sub@xxxxxxxxxxxxx>> sub.

=====

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@xxxxxxxxxxxxx

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

=====

=====

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.