

[NT] Account Theft Vulnerability in MakeBid Auction Deluxe

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-02/0090.html>

From: support@securiteam.com

Date: 02/15/02

From: support@securiteam.com

To: list@securiteam.com

Date: Fri, 15 Feb 2002 22:20:24 +0100 (CET)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Account Theft Vulnerability in MakeBid Auction Deluxe

SUMMARY

MakeBid Auction Deluxe is a commercial PERL CGI that allows web users to add items to an online auction. The following fields are not properly sanitized when placing a new item on auction:

- + City/State/Zip of new auction registrant
- + Title Description of new auction item
- + Item Description for new auction item

This allows an attacker to place an item on auction with potentially malicious code in the description fields. This code will be executed on clients' browsers when viewing the items, and allows attackers to steal the authentication cookie and therefore gain access to the target's account.

DETAILS

Vulnerable systems:

MakeBid Auction Deluxe version 3.30

MakeBid Auction Deluxe has the option of allowing the user to store their login credentials in a cookie. These credentials are stored in clear text.

Securiteam: [NT] Account Theft Vulnerability in MakeBid Auction Deluxe

In conjunction, these two vulnerabilities allow an attacker to steal the accounts of any auction participant that utilizes the "save login" option. An attacker can use the compromised account to place unauthorized bids, place items on auction as other users, and modify contact and payment information. This vulnerability also allows the attacker to gather personal information and partial credit card data from the affected accounts.

Vendor status:

Vendor has been contacted via email and a patch for the cross-site scripting vulnerability is available for registered users. Cookies are still stored in clear text.

ADDITIONAL INFORMATION

The information has been provided by <mailto:blake@mc.net> Blake Frantz.

=====

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

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

-
- **Previous message:** support@securiteam.com: "[NT] Buffer Overflow Found in MSHTML.DLL"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)