

[UNIX] Sun Secure Global Desktop Multiple Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-09/msg00032.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 21 Sep 2006 13:41:42 +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>

Sun Secure Global Desktop Multiple Vulnerabilities

SUMMARY

<<https://sgddemo.sun.com/>> Sun Secure Global Desktop (SSGD, formerly known as Tarantella[1]) is "an open-source remote desktop solution with a basic amount of security". Marc Ruef at scip AG found six undisclosed web-based vulnerabilities in Sun Secure Global Desktop prior 4.3.

DETAILS

1. Cross site scripting

Some scripts that are not protected by any authentication procedure can be used to run arbitrary script code within a cross site scripting attack.

2. Revealing of sensitive information

Some scripts that are not protected by any authentication procedure can be accessed to reveal sensitive information (e.g. internal hostnames, applied software version, details about settings) about the target host.

Exploitation:

Classic script injection techniques and unexpected input data within a browser session can be used to exploit these vulnerabilities.

[UNIX] Sun Secure Global Desktop Multiple Vulnerabilities

Impact:

Because non-authenticated parts of the software are affected, these vulnerabilities are serious for every secure environment.

Non-authenticated users might be able to exploit the flaws to gain elevated privileges (e.g. extracting sensitive cookie information or launch a buffer overflow attack against another web browser).

Solution:

We have informed Sun on a very early stage. They said that the problems will be addressed with a bugfix for the currently shipping version 4.2 and will no longer be existing in the upcoming version 4.3. We were told that the public release for the patch is at the end of August 2006. Due to no public release was made and our last emails were not answered, we do not know what kind of official solution is available. This is why we are not going to publish any technical details or exploits at the moment.

De-activate the following scripts to gain a higher level of security:

- ttaarchives.cgi
- ttaAuthentication.jsp
- ttalicense.cgi
- ttawlogin.cgi
- ttawebtop.cgi
- ttaabout.cgi
- test-cgi

Vendor Response:

Sun Microsystems Inc. has been informed a first time at 07/04/2006 via email to contactus-at-sun.com. Because no reply came back we decided to send a forwarding at 07/18/2006 to security-alert-at-sun.com. A first response came back on the same day. Several email messages were exchanged to discuss the vulnerabilities and to co-ordinate the disclosure of this advisory. However, the last emails since 09/15/2006 have not been answered.

Disclosure Timeline:

06/06/06 Identification of the vulnerabilities
07/04/06 First information to contactus-at-sun.com
07/18/06 Second information to security-alert-at-sun.com
09/15/06 Sending the last email which is still unanswered
09/21/06 Public disclosure of this advisory

ADDITIONAL INFORMATION

The information has been provided by <<mailto:maru@xxxxxxx>> Marc Ruef.

The original article can be found at:

<<http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=2555>>

<http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=2555>

[UNIX] Sun Secure Global Desktop Multiple Vulnerabilities

=====

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@xxxxxxxxxxxxxxxx

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

=====

=====

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.