

[NT] First Security Agent and First Screen Lock Package Vulnerability (Bypassing, Disabling)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-07/0042.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 07/08/03

To: list@securiteam.com

Date: 8 Jul 2003 14:17:30 +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

Beyond Security in Canada

Toronto-based Sunrays Technologies is now Beyond Security's representative in Canada.

We welcome ISPs, system integrators and IT systems resellers

to promote the most advanced vulnerability assessment solutions today.

Contact us at 416-482-0038 or at canadasales@beyondsecurity.com

First Security Agent and First Screen Lock Package Vulnerability
(Bypassing, Disabling)

SUMMARY

<<http://www.softheap.com/>> 1st Security Agent is "an excellent password-protected security utility to secure Windows-based computers. It works under any Windows platform and offers an administrative support for controlling which users are allowed to access your computer and the level of access each user may have". A vulnerability in two of the company's products allows local attackers to bypass the product, or disable it, by access certain keys that have not been properly protected.

DETAILS

Description of Vulnerability:

1st Security Agent stores its password settings by default under the

Registry Key:

HKEY_LOCAL_MACHINE\SOFTWARE\SaSkda

Securiteam: [NT] First Security Agent and First Screen Lock Package Vulnerability (Bypassing, Disabling)

It stores two vulnerable settings by default:

LockPwd – stores the passwords in plaintext (Un-encrypted) and writeable.

LockPwdEnabled – stores the value writeable (Modifiable) by all users.

With these two Settings, a user can either:

- a.) Read the password set by a user, potentially leading to further compromise of the system if the password is used more than once.
- b.) Change the password to restrict other users from their machines.
- c.) Disable Screen Lock.

Example:

Setup screen lock, enter a default password and open up the Registry keys folder. You will see your specified password in plaintext in the LockPwd key. Right click on LockPwd and select modify, change the value from the password you specified and try unlocking your screen. The new password is the effective one.

Right Click LockPwdEnabled and change the Value Data to 0, run the screen lock and you will not need a password to continue.

Fix:

Until the vendor releases a patch for these vulnerabilities, you should modify user access privileges, disabling registry editing, and change the world writeable specifications to something such as Administrator. Isolate your default password, meaning use something that you don't use for other applications, this will prevent further privilege escalation.

ADDITIONAL INFORMATION

The information has been provided by <mailto:mercy@dtors.net> mercy.

=====

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.