

[NT] KGB Key Logger Password Protection Bypass

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-01/msg00012.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 4 Jan 2006 17:51:12 +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>

KGB Key Logger Password Protection Bypass

SUMMARY

" <<http://refog.com/free-keylogger/key-logger.html>> KGB Free Keylogger is a program intercepting keystrokes (that is, a key logger)."

By modifying the INI file of KGB Key Logger local attackers can bypass the password and executing KGB Key Logger.

DETAILS

Vulnerable Systems:

- * KGB Key Logger 1.93

KGB Key Logger password is stored on "C:\Document And Settings\All Users\Application data\KSP"

Allowing every user on the system to change, add and modify the Password, Question and Answer.

Alto the password by itself is encrypted, users can change the passwords, see the question and answer, and generate a new password, or just change the settings.

[NT] KGB Key Logger Password Protection Bypass

KGP.INI

..

[Password]

OldPassword=E2390F050F1C3DDA3534A73D2ADF45FF

Question=

Answer=

..

ADDITIONAL INFORMATION

The information has been provided by

<<mailto:iman.karim@xx>> imax.

=====

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.



- Prev by Date: [**\[NT\] Vulnerability in Graphics Rendering Engine Allows Remote Code Execution**](#)
- Next by Date: [**\[NEWS\] Sony's Instant Video Everywhere Service Replay Attack**](#)
- Previous by thread: [**\[NT\] Vulnerability in Graphics Rendering Engine Allows Remote Code Execution**](#)
- Next by thread: [**\[NEWS\] Sony's Instant Video Everywhere Service Replay Attack**](#)
- Index(es):
 - ◆ [**Date**](#)
 - ◆ [**Thread**](#)