

[UNIX] Multiple Vulnerabilities in Konversation

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-01/0094.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 01/23/05

To: list@securiteam.com

Date: 23 Jan 2005 14:28:44 +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>

Multiple Vulnerabilities in Konversation

SUMMARY

Multiple vulnerabilities have been discovered in Konversation, an IRC client for KDE.

A flaw in the expansion of %-escaped variables makes that %-escaped variables in certain input strings will be inadvertently expanded too. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2005-0129 to this issue.

Several perl scripts included with Konversation fail to properly handle command line arguments causing a command line injection vulnerability. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2005-0130 to this issue.

Nick and password are confused in the quick connection dialog, so connecting with that dialog and filling in a password, would use that password as nick, and may inadvertently expose the password to others. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2005-0131 to this issue.

DETAILS

Securiteam: [UNIX] Multiple Vulnerabilities in Konversation

Vulnerable Systems:

- * Konversation versions up to and including 0.15

Immune Systems:

- * Konversation version 0.15.1 or newer

Impact:

A user might be tricked to join a channel with a specially crafted channel name containing shell commands. If user runs a script in that channel it will result in an arbitrary command execution.

If quick connect is used with a password, the password is used as nickname instead. As a result the password may be exposed to others.

Patch:

A patch for Konversation 0.15 is available from

<ftp://ftp.kde.org/pub/kde/security_patches>

ftp://ftp.kde.org/pub/kde/security_patches

CVE Information:

<<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0129>>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0129>

<<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0130>>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0130>

<<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0131>>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0131>

Time line and credits:

18/01/2005 Konversation developers informed by Wouter Coekaerts

19/01/2005 Patches applied to KDE CVS

19/01/2005 Konversation 0.15.1 released

21/01/2005 KDE Security Advisory released

ADDITIONAL INFORMATION

The information has been provided by <<mailto:bastian@kde.org>> Waldo Bastian.

=====

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,

Securiteam: [UNIX] Multiple Vulnerabilities in Konversation

loss of business profits or special damages.