

[EXPL] Multiple Vulnerabilities in Konversation (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-01/0104.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 01/23/05

To: list@securiteam.com

Date: 23 Jan 2005 17:14:59 +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 (Exploit)

SUMMARY

Multiple vulnerabilities have been discovered in Konversation, an IRC client for KDE. One allows execution of arbitrary commands via the % expansion mechanism, another allows execution of arbitrary commands via the command line support scripts. The following two proof of concepts can be used to test your system for the mentioned vulnerability.

DETAILS

Vulnerable Systems:

* Konversation version 0.15.0 and prior

Immune Systems:

* Konversation version 0.15.1 or newer

% Expanding

Konversation's Server::parseWildcards function contains a vulnerability that allows a remote attacker to utilize its expanding '%' feature to cause it to execute arbitrary code.

Securiteam: [EXPL] Multiple Vulnerabilities in Konversation (Exploit)

Example:

Utilizing the following channel name `#%n/quit%n` will cause a receiving an invitation to this channel to exit Konversation.

Included Perl Scripts Vulnerable to Shell Command Injection

Perl scripts included with Konversation execute a commands line similar to:

```
exec ("dcop $PORT Konversation say $SERVER \"$TARGET\" output");
```

Where the shell characters in `$SERVER` or `$TARGET` aren't escaped.

Example:

Therefore, joining a channel named `#`kwrite`` and executing the sample script (for example typing `/uptime`) will start `kwrite`.

Solution:

These problems are fixed in version 0.15.1, which was released 19/01/05

Individual patches can be downloaded at:

<<http://wouter.coekaerts.be/files/konversation-parse.diff>>

<http://wouter.coekaerts.be/files/konversation-parse.diff>

<<http://wouter.coekaerts.be/files/konversation-quickconnect.diff>>

<http://wouter.coekaerts.be/files/konversation-quickconnect.diff>

<<http://wouter.coekaerts.be/files/konversation-scripts.diff>>

<http://wouter.coekaerts.be/files/konversation-scripts.diff>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:wouter@coekaerts.be>> Wouter Coekaerts.

The original article can be found at:

<<http://wouter.coekaerts.be/konversation.html>>

<http://wouter.coekaerts.be/konversation.html>

=====

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.