

[UNIX] KDE URI handler vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-05/0062.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 05/18/04

To: list@securiteam.com

Date: 18 May 2004 18:26:55 +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>

KDE URI handler vulnerabilities

SUMMARY

A bug in KDE can be used by an attacker to create or truncate arbitrary files in any location the user has permissions to do so by specifying a non-valid URI. The KDE URI handler does not perform adequate filtering which give rise to the problem.

DETAILS

Vulnerable Systems:

- * KDE versions 3.2.2 and prior

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0411>>
CAN-2004-0411

The Telnet, rlogin, SSH and mailto URI handlers in KDE do not check for '-' at the beginning of the hostname passed, which makes it possible to pass an option to the programs started by the handlers.

Impact

* A remote attacker could entice a user to open a carefully crafted telnet URI which may either create or truncate a file anywhere where the

Securiteam: [UNIX] KDE URI handler vulnerabilities

victim has permission to do so. In KDE 3.2 and later versions the user is first explicitly asked to confirm the opening of the telnet URI.

* A remote attacker could entice a user to open a carefully crafted mailto URI which may start the KMail program with its display redirected to a remote machine under control of the attacker. An attacker can then use this to gain full access to the victim's personal files and account.

* An attacker could entice a user to open a carefully crafted mailto URI which may start the KMail program using a configuration file specified by the attacker. If the attacker is able to install arbitrary files somewhere on the machine, the attacker can include commands in the configuration file that will be executed with the privileges of the victim allowing the attacker to gain full access to the victims personal files and account.

Patch Availability:

Source code patches and updated binary packages are available where appropriate. In order to mitigate this vulnerability users are advised to upgrade their version of the vulnerable packages (information can be obtained from specific vendors).

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, loss of business profits or special damages.