

[UNIX] Evolution Multiple Format String Vulnerabilites

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-08/0063.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/14/05

To: list@securiteam.com

Date: 14 Aug 2005 18:02:38 +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>

Evolution Multiple Format String Vulnerabilites

SUMMARY

Evolution suffers from several format string bugs when handling data from remote sources. These bugs lead to crashes or the execution of arbitrary assembly language code.

DETAILS

Vulnerable Systems:

- * Evolution version 1.5
- * Evolution version 2.0
- * Evolution version 2.1
- * Evolution version 2.2
- * Evolution version 2.3

Immune Systems:

- * Evolution version 2.3.7 or newer

1) The first format string bug occurs when viewing the full vCard data attached to an e-mail message.

Securiteam: [UNIX] Evolution Multiple Format String Vulnerabilites

When opening an e-mail message, only a compact view of some of the fields from the vCard is displayed, and this does not trigger the vulnerability. To be affected, the user must click on Show Full vCard or perform similar actions such as clicking on Save in Addressbook and then viewing the saved data under the Contacts tab.

Why is this important? An attacker might notice that an organisation uses Evolution, for instance after seeing the "X-Mailer: Evolution x.y.z" e-mail header in their e-mails. He or she could then send out e-mail messages with malicious vCards to many e-mail accounts at the organisation, in the hope that some of the recipients will view the full vCard data sooner or later, thus exposing the organisation to this format string bug.

2) The second format string bug occurs when displaying contact data from remote LDAP servers.

3) The third format string bug occurs when displaying task list data from remote servers.

4) The fourth, and least serious, format string bug occurs when the user goes to the Calendars tab to save task list data that is vulnerable to problem 3 above. Other calendar entries that do not come from task lists are also affected.

Mitigating factors:

* Users that never use any of the vulnerable features in Evolution are not affected.

Recommendations:

We recommend that users either upgrade to Evolution 2.3.7 (unstable) or apply our unofficial patch to their Evolution installation.

Patch information:

Evolution 2.3.7 is available from the following source:

<<http://ftp.gnome.org/pub/gnome/sources/evolution/>>

<http://ftp.gnome.org/pub/gnome/sources/evolution/>

Our unofficial patch is available from the following page:

<<http://www.sitic.se>> <http://www.sitic.se>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:sitic@pts.se>> SITIC Vulnerability Advisory.

=====

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

Securiteam: [UNIX] Evolution Multiple Format String Vulnerabilites

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.