

Evolution Mailer DoS

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2006-03/msg00022.html>

- *From:* Alan Cox <alan@xxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 1 Mar 2006 16:58:40 +0000
-

About 7 weeks ago an automated mailing list spewed a large but valid email containing a lot of URLs and other formatting. When this email is fed into evolution the behaviour it causes leads evolution to expand dramatically in size and eat vast amounts of CPU time. If you've got a lot of patience and memory it is eventually rendered correctly (many minutes and many gigs)

The attack in question can be triggered with a large but valid plain text email containing no unusual features. It is possible to perform the attack with a somewhat smaller message than the one given but the one provided should suffice for analysis and testing.

Worse, and the reason this becomes more than irritating is that evolution tries to be smart when it is killed or dies. On restarting it will go to great trouble to attempt to restart in the same position it died or was shut down – which triggers the DoS again each time evolution is opened.

This bug was reported to vendor–sec January 18th, and acknowledged January 19th as CVE–2006–0040. A request for any follow up details was posted end of February. No vendor has chosen to provide any more information which I find disappointing.

The email that triggered the original accidental discovery is available at

<http://zeniv.linux.org.uk/~alan/destroy-evolution.mbox>

As the problem appears to come from gtkhtml it is likely that other gtkhtml users may be similarly afflicted.

Recommendations:

Block large text emails with many URLs using a filter rule
Ask your vendor awkward questions
or switch mailer

Happy St Davids Day
Alan