

ScatterChat Advisory 2006-01: Cryptanalytic Attack Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2006-08/msg00258.html>

- *From:* "ScatterChat Advisories" <sc_advisories@xxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 11 Aug 2006 10:25:52 -0400 (EDT)
-

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

ScatterChat Advisory 2006-01: Cryptanalytic Attack Vulnerability
Technical Report
CVE ID: CVE-2006-4021
August 11th, 2006
<http://www.scatterchat.com/>

SUMMARY

ScatterChat (<http://www.scatterchat.com/>) is an instant messaging project that aims to provide encryption and anonymity support with Tor to non-technical users such as human rights activists and political dissidents.

Steven Murdoch, a security researcher with the University of Cambridge, discovered a theoretical weakness in ScatterChat's cryptographic module. He found that an eavesdropper might locate patterns in a private communications channel if extraordinarily large amounts of messages were exchanged in a single conversation.

Note that this does not allow an eavesdropper to decrypt messages, nor determine a user's identity if anonymity is used.

The practical impact of this vulnerability is very low.

DETAILS

It was found that the birthday attack could be used against the custom padding mechanism on the ECB-mode encryption of messages.

After 114KB of data is sent in a single conversation the probability of a collision between two 16-byte blocks is 1% and will reach 50%

ScatterChat Advisory 2006–01: Cryptanalytic Attack Vulnerability

after 904KB, then 99% after 2.3MB (approximately). Note that conversations are reset when one or both peers sign off from the instant messaging service.

The above figures are calculated assuming that messages do not contain any entropy, which is unrealistic for an instant messaging environment. Assuming a rate of one bit of entropy per character, the probability of a collision is 1% after 580KB is exchanged and will reach 50% after 4,822KB, then 99% after 12,431KB (approximately).

Note that if each instant message was filled to its 500–byte capacity (as enforced by the system), then 580KB would be transferred after 1,188 messages.

IMPACT

The end–user impact of this issue is very low.

It is important to note that this issue does NOT allow an eavesdropper to decrypt any messages, nor does it allow them to discover the user's identity if the anonymity feature is used.

In general, this type of cryptanalytic attack allows an eavesdropper to determine patterns in an encrypted conversation, which in theory could yield information about messages if enough patterns were found and correlated. However, this issue only allows two 16–byte segments to be matched with 1% probability when at least 1,188 instant messages are exchanged in a single, uninterrupted session. In most cases, more than 1,188 instant messages would need to be sent.

The information leaked in the above situation would be negligible.

This issue also affects any application that is built upon ScatterChat's encryption module.

Note that secure file transfers are not affected.

SOLUTION

The ScatterChat project takes both practical and theoretical vulnerabilities very seriously. However, due to the low impact of this vulnerability, and the high risk of introducing other subtle security problems in updating the protocol, this issue will not be fixed in the v1.0.x branch.

This issue will be rectified in the v2.0 series, which will replace the current cryptographic module with the well–tested OTR encryption

ScatterChat Advisory 2006-01: Cryptanalytic Attack Vulnerability

module (<http://www.cypherpunks.ca/otr/>). A release date for v2.0 is not yet known.

Optionally, this issue can be mitigated through the use of the anonymity feature, as traffic analysis often requires a known context to make sense of patterns. Without the knowledge of who is communicating, an eavesdropper's attempts at interpreting patterns can be frustrated.

ScatterChat v1.0.x remains safe to use in the overwhelming majority of cases. However, for high risk, non-technical users, i.e., users operating behind national firewalls, we recommend extra caution.

ACKNOWLEDGEMENTS

A special thanks goes out to Steven Murdoch for his professionalism in dealing with this matter. His web page can be found at:
<http://www.cl.cam.ac.uk/users/sjm217/>

CONTACT

J. Salvatore Testa II
jtesta--at--hactivismo--dot--com

http://www.scatterchat.com/jtesta_2006.asc
3428 E58E 715E C37D 2AA7 C55E 97D1 DE8C 4B26 2B62

--

A less technical summary of this advisory can be found at:
http://www.scatterchat.com/advisories/2006-01_non_tech.html

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.5 (GNU/Linux)

iD8DBQFE3H6119HejEsmK2IRAsEtAJ9kX3PDigpPb+aaPWlfQ5IqwyskYgCgiKZ2
Kf0CYKzvc80KAKtBkT7zVgc=
=335D

-----END PGP SIGNATURE-----