CERT Incident Note IN-2000-08: Chat Clients and Network Security

The CERT Coordination Center publishes incident notes to provide information about incidents to the Internet community.

Chat Clients and Network Security

Date: Wednesday, June 21, 2000

The CERT/CC has received reports and inquiries regarding the security issues inherent in the use of chat clients.

Internet chat applications, such as instant messenging applications and Internet Relay Chat (IRC) networks, provide a mechanism for information to be transmitted between computers within a network and computers at remote sites across network borders in both directions. Chat clients provide groups of individuals the means to exchange dialog, Web URL's, and in many cases, files of any type. As with any similar networked application (e.g., email), chat applications pose security risks when used in a networked environment.

The security model of chat clients is one that relies on each end-user to make independent security decisions rather than relying on a central enforceable security policy. The result is a broader base of exposure to risk across a network with less central control, making security policies that allow chat client usage difficult to implement and enforce.

There are several general security issues network and system administrators can consider when evaluating security policies and the use of chat clients.

- Software flaws, such as buffer overflows or insecure configurations, may be present in client software and may provide a means for remote users to initiate attacks that execute code on internal systems. The configuration of chat software should be reviewed; check security settings and insure security issues have been addressed with work arounds or patches.
- Social engineering attacks may entice users into taking insecure actions, such as communicating sensitive information with outsiders or executing untrusted software. Users should be aware of the potential for social engineering attacks and use caution in releasing information and executing untrusted software.
- Information, including passwords, may be passed across untrusted networks (both domestic and international) in clear text, making them subject to interception. Strong encryption, if available, should be used to secure sensitive communications.
- For sensitive communications, it may be difficult to strongly authenticate the identity of remote parties using only the information provided in most chat clients. Strong authentication, if available, should be used to establish trusted communications.
- Attacks involving Trojan horse programs have been known to leverage chat networks to enable intruders to coordinate the actions of compromised computers in attacks against other Internet sites.

A general security practice for system configuration is to disable all services that are not needed. The same concept can be applied to network configuration. Unless the services provided by chat clients are needed in your environment, we encourage you to consider disabling chat client functionality on your network.

Author: Kevin Houle