Netscape Navigator 1.12 (Macintosh)

****
  IMPORTANT! Before going any further, please
 read and accept the terms in the file LICENSE.
****

Release notes for this version of Netscape Navigator are available online. After starting the program, select "Release Notes" from the "Help" menu. This will take you to the URL

  http://home.netscape.com/eng/mozilla/1.1/relnotes/mac-1.12.html

which lists new features and known problems of this release.

To submit bugs or other feedback, use the "How To Give Feedback" option, also on the "Help" menu, which will take you to the URL

  http://home.netscape.com/home/how-to-give-feedback.html

If for some reason you cannot submit feedback using that form, you may send email to mac_cbug@netscape.com. Please be as specific as possible about the version of Netscape you are using, and the hardware and version of the OS. If possible, include a test case for the problem, including a URL.

========== Security Fix Description ==========
TECHNICAL BACKGROUND

Netscape Navigator uses random information to generate session encryption keys of either 40 or 128 bits in length. The random information is found through a variety of functions that look into a user's machine for information about how many processes are running, process ID numbers, the current time in microseconds, etc. Previous releases of Netscape Navigator were vulnerable because the size of random input was less than the size of the subsequent keys. This means that instead of searching through all the 2^128 possible keys by brute force, a potential intruder only had to search through a significantly smaller key space by brute force. This was a substantially easier problem to solve because it takes much less compute time and means 40-bit or 128-bit key strength is substantially reduced.

SOLUTION

Netscape Navigator 1.12 (Macintosh) fixes the specific portion of our software where this vulnerability existed. We have significantly increased the amount of random information that cannot be discovered by external sources from approximately 30 bits to approximately 300 bits.

Netscape has greatly expanded the techniques and sources used to generate the random information. The number of unpredictable bits in the RNG makes it no longer the weak link in the chain.

==========
Installation Instructions
==========

This version of Netscape comes with an installer which will let you choose between 68000, PowerPC and FAT binaries of Netscape.

Installation Steps:

1) Download the .HQX file to your Macintosh. If you are using Netscape to do the download and your machine is correctly configured, Netscape will automatically run the correct program to decode the .HQX file. If not, you wil need to use one of the many utilities which can decode .HQX files (Binhex format), we recommend something in the StuffIt family of products, such as "StuffIt Expander"

2) To install Netscape, double click the installer named "Netscape 1.12 Installer".

a) Press "Install" to get a binary which matches your Macintosh CPU.

b) To install a FAT binary which will run on all Macintoshes, select "Custom Install" by pulling down the menu in the upper left corner of the installer window, and then press the "Install" button.

3) Remember to read the release notes mentioned above. They contain helpful and up-to-date information about running this version of Netscape.