

SecurityFocus Bugtraq: Opera directory traversal and buffer overflow

must pass some checks to assure Opera of it being a real zip file. The file extension can be chosen arbitrarily by the attacker.

One exploit scenario is to place a zip-like file in the victim user's Startup folder. The file extension determines how it will be opened by Windows. E.g. if the file name ends with ".bat", it will be opened as a batch file. It's relatively easy to create a file which passes the check as zip file but also works when opened as a batch file. Due to the zip file signature and other binary data it will produce some error messages but nevertheless command lines contained in the file will be executed. In this way an attacker can get access to the system with the privileges of the current user.

Locating the Startup folder isn't a problem because Opera's skin folder is below the %