



## Full-Disclosure: [Full-Disclosure] Opera directory traversal and buffer overflow

As the browser doesn't accept just any file after the 7.22 update, exploiting the issue becomes slightly more difficult. The file format 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 %USREPROFILE% folder, and pointing to the startup folder with a relative path is easy.

The zip processing code also contains a buffer overflow which I found while testing the abovementioned vulnerability. If a valid zip file contains extra data after the zip data, a buffer overflow occurs. An attacker may control contents of some registers including EIP, so this buffer overflow seems exploitable, although I didn't produce an exploit.

In order to be exploited, these vulnerabilities require the victim to visit a web page created by a malicious user. An iframe tag may be used to automatically open a skin file.

The directory traversal problem doesn't exist on Linux because "\" isn't a directory separator. Other versions weren't tested. The buffer overflow can be produced on Linux, too.

### VENDOR STATUS

=====

The vendor was notified on November 12, 2003 and a new version of Opera was released on November 21st. It can be downloaded at

<ftp://ftp.opera.com/pub/opera/>

### CREDITS

=====

The vulnerabilities were discovered by Jouko Pynnönen, Finland.

--

Jouko Pynnönen  
jouko@iki.fi

Web: <http://iki.fi/jouko/>  
GSM: +358 41 5504555

---

Full-Disclosure - We believe in it.

## Full-Disclosure: [Full-Disclosure] Opera directory traversal and buffer overflow

Charter: <http://lists.netsys.com/full-disclosure-charter.html>