

Opera Telnet URI Handler File Creation/Truncation Vulnerability

IDEFENSE Security Advisory 05.12.04:

I. BACKGROUND

Opera is a cross-platform web browser. More information is available from <http://www.opera.com/>

II. DESCRIPTION

Exploitation of an input validation vulnerability within Opera Software ASA.'s Opera Web Browser could allow remote attackers to create or truncate arbitrary files.

The problem specifically exists within the telnet URI handler. Opera does not check for '-' at the beginning of hostname passed through the handler, which lets options pass to the telnet program, allowing file creation or overwriting. Under Windows XP, when telnet.exe is executed with the '-f' option, the remainder of the argument is used as a filename for logging the connection. Under Linux, the '-n' option creates a 'tracefile' for the connection. These options create a file if it does not exist, or truncates it if it does.

If a telnet: URI with the appropriate option is opened, a file will be created in the current working directory of the Opera process if the user has permission. In Windows, this defaults to the directory Opera was installed in. Under Linux, the default is the user's home directory.

Examples:

Windows XP: Creates or overwrites 'Filename' in Opera directory.

```
telnet://-fFileName
```

Under Linux: Creates or overwrites 'Filename' in user's home directory.

```
telnet://-nFilename
```

Under some previous versions of Opera, it was possible to create a file anywhere on the filesystem, by hex encoding an absolute path in the filename portion of the URI.

III. ANALYSIS

In Windows, depending on the privileges, it may be possible to make Opera unavailable by overwriting files. Under Linux it is possible to overwrite files in the current user's home directory (e.g. .bashrc, mbox)

Some versions or configurations of Windows may not be vulnerable, due to the absence of the '-f' command line switch.

IV. DETECTION

Opera 7.23 has been confirmed vulnerable, as have a variety of earlier versions on multiple platforms. It is suspected that all earlier versions are also vulnerable.

V. WORKAROUNDS

Disable the telnet URI handler from within Opera.

Click on the 'File' menu, then the 'Preferences...' item choose 'Programs and paths' from the view on the left. Select on 'telnet' from the Protocols box and press the delete key. Do the same with the tn3270 handler.

VI. VENDOR RESPONSE

The vulnerability has been addressed in Opera 7.50 (Windows, Mac, Linux).

Windows version downloadable from

<http://www.opera.com/download/index.dml?opsys=Windows&platform=Windows&lng=en&ver=7.50>

Mac version downloadable from

<http://www.opera.com/download/index.dml?step=3&opsys=MacOS&lng=en&platform=MacOS>

Linux i386 version downloadable from

<http://www.opera.com/download/index.dml?step=3&opsys=Linux%20i386&lng=en&platform=Linux%20i386>

VII. CVE INFORMATION

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CAN-2004-0473 to this issue. This is a candidate for inclusion in the CVE list (<http://cve.mitre.org>), which standardizes names for security problems.

VIII. DISCLOSURE TIMELINE

April 2, 2003	Exploit acquired by iDEFENSE
April 7, 2004	Initial vendor notification
April 7, 2004	iDEFENSE clients notified
April 14, 2004	Initial vendor response
May 12, 2004	Coordinated public disclosure

IX. CREDIT

Karol Wieseck and Greg MacManus are credited with this discovery.