

[VulnWatch] Secunia Research: Opera browser Cross Site Scripting

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2003-02/0045.html>

From: Jakob Balle (jb@secunia.com)

Date: 02/26/03

From: Jakob Balle <jb@secunia.com>

To: vulnwatch@vulnwatch.org

Date: 26 Feb 2003 10:24:20 +0100

Secunia Research 26/02/2003

– Opera browser Cross Site Scripting –

Table of Contents

1.....	Description
2.....	Affected Software
3.....	Severity
4.....	Exploit
5.....	Solution
6.....	Time Table
7.....	About Secunia
8.....	Credits
9.....	Verification

1) Description

A vulnerability exists in the way the Opera browser generates a temporary page for displaying a redirection, when "Automatic redirection" is disabled (not default setting).

When Opera generates a page for displaying a redirect, it does not strip any characters, making it possible to inject malicious script code into the page generated by the Opera browser. This page has the same privileges as the domain trying to redirect the user, making it possible to steal cookies, hi-jack sessions etc. from the domain.

Eg. many websites use a "redirect-script" to redirect users. These scripts often take arguments without any further validation, because

their only function is to send the user to a new URL. However, when Opera is set to not automatically redirect a user, Opera will display this URL on a temporary page without stripping it for malicious code.

2) Affected Software

Following have been tested and found vulnerable:

Opera prior to 7.02 on Windows

Opera 6.x on Linux

Vendor:

<http://www.opera.com/>

3) Severity

Rating: Less critical

Impact: Cross Site Scripting

Where: From Remote

4) Exploit

Sample exploit:

http://www.secunia.com/secunia_research/2003-1/exploit/

5) Solution

Vendor patch:

Windows: Update to latest version. Opera v7.02 is not vulnerable.

Linux: No update available.

Workaround:

A workaround would be to leave "Automatic redirection" enabled.

6) Time Table

15/02/2003 – Vulnerability discovered

16/02/2003 – Further research

17/02/2003 – Vendor informed

19/02/2003 – Vendor confirmed and fixed vulnerability

26/02/2003 – Vendor released Opera v7.02

26/02/2003 – Public disclosure of vulnerability

7) About Secunia

Secunia collects, validates, assesses and writes advisories regarding all the latest software vulnerabilities disclosed to the public. These advisories are gathered in a publicly available database at the Secunia website:

<http://www.secunia.com/>

Secunia offers services to our customers enabling them to receive all relevant vulnerability information to their specific system configuration.

=====

8) Credits

Jakob Balle, Secunia

=====

9) Verification

Please verify this advisory by visiting the Secunia website.

http://www.secunia.com/secunia_research/2003-1/

=====