Apple Safari Multiple Vulnerabilities

2008-03-20 01:36:44 by Raven

SECUNIA ADVISORY ID: SA29393

VERIFY ADVISORY: http://secunia.com/advisories/29393/

CRITICAL: Highly critical

IMPACT: Security Bypass, Cross Site Scripting, Exposure of sensitive information, System access

SOFTWARE:
Safari 3.x - http://secunia.com/product/17989/
Safari 2.x - http://secunia.com/product/5289/

DESCRIPTION: Some vulnerabilities have been reported in Safari, which can be exploited by malicious people to bypass certain security restrictions, conduct cross-site scripting attacks, or to compromise a vulnerable system. The vulnerabilities are reported in Safari prior to version 3.1.

1) An error in the processing of "javascript:" URLs can be exploited to execute arbitrary HTML and script code in context of another site via a specially crafted web page.

2) An error exists the handling of web pages that have explicitly set the document.domain property. This can be exploited to conduct cross-site scripting attacks in sites that set the document.domain property or between HTTP and HTTPS sites with the same document.domain.

3) An error in Web Inspector can be exploited to inject script code that will run in other domains and can read the user's file system when a specially crafted page is inspected.

4) A security issue exists with the Kotoeri input method, which can result in exposing the password field on the display when reverse conversion is requested.

5) An error within the handling of the "window.open()" function can be used to change the security context of a web page to the caller's context. This can be exploited to execute arbitrary script code in the user's security context via a specially crafted web page.

6) The frame navigation policy is not enforced for Java applets. This can be exploited to conduct cross-site scripting attacks using java and to gain escalated privileges by enticing a user to open a specially crafted web page.

7) An unspecified error in the handling of the document.domain property can be exploited to conduct cross-site scripting attacks when a user visits a specially crafted web page.

8) An error exists in the handling of the history object. This can be exploited to inject javascript code that will run in the context of other frames.

9) A boundary error exists in the handling of javascript regular expressions, which can be exploited to cause a buffer overflow via a specially crafted web page. Successful exploitation allows execution of arbitrary code.

10) An error in WebKit allows method instances from one frame to be called in the context of another frame. This can be exploited to conduct cross-site scripting attacks.

SOLUTION: Update to version 3.1.

PROVIDED AND/OR DISCOVERED BY:
1) Robert Swiecki of Google Information Security Team
2, 3, 5, 6) Adam Barth and Collin Jackson of Stanford University
10) Eric Seidel of the WebKit Open Source Project, and Tavis Ormandy and Will Drewry of Google Security Team

ORIGINAL ADVISORY: Apple: http://docs.info.apple.com/article.html?artnum=307563

https://www.ravenphpscripts.com/modules.php?name=News&file=article&sid=3277