

[Full-disclosure] Google Chrome 0.2.149.27 'SaveAs' Function Buffer Overflow Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2008-09/msg00114.html>

- *From:* "SVRT" <svrt@xxxxxxxxxxxxx>
 - *Date:* Fri, 05 Sep 2008 20:12:49 +0700
-

We (SVRT-Bkis) have just discovered vulnerability in Google Chrome 0.2.149.27. This is a Critical Buffer Overflow Vulnerability permitting hacker to perform a remote attack and take complete control of the affected system.

We have submitted this Vulnerability to Google. They confirmed and assign a verifier for build 0.2.149.28.

Proof of Concept:

We tested Google Chrome 0.2.149.27 on Windows XP SP2 (Open Calculator)

<http://security.bkis.vn/Proof-Of-Concept/PoC-XPSP2.html>

With others Windows not XP SP 2:

<http://security.bkis.vn/Proof-Of-Concept/PoC-Crash.html>

Details:

- Type of Issue : Buffer Overflow.
- Affected Software : Google Chrome 0.2.149.27.
- Exploitation Environment : Google Chrome on Windows XP SP2.
- Impact: Remote code execution.
- Rating : Critical.
- Description :
The vulnerability is caused due to a boundary error when handling the SaveAs function. On saving a malicious page with an overly long title (<title> tag in HTML), the program causes a stack-based overflow and makes it possible for attackers to execute arbitrary code on users systems.
- How an attacker could exploit the issue :
To exploit the Vulnerability, a hacker might construct a specially crafted Web page, which contains malicious code. He then tricks users into visiting his Website and convinces them to save this Page. Right after that, the code would be executed, giving him the privilege to make use of the affected system.

[Full-disclosure] Google Chrome 0.2.149.27 'SaveAs' Function Buffer Overflow Vulnerability

– Discoverer : Le Duc Anh – SVRT – Bkis

– About SVRT :

SVRT, which is short for Security Vulnerability Research Team, is one of Bkis researching groups. SVRT specializes in the detection, alert and announcement of security vulnerabilities in software, operating systems, network protocols and embedded systems&

– About Bkis :

Bkis (Bach Khoa Internetwork Security) is Vietnamese leading Center in researching, deploying network security software and solutions.

– Website : <http://security.bkis.vn>

– Mail : [svrt\[at\]bkav.com.vn](mailto:svrt[at]bkav.com.vn)

Full-Disclosure – We believe in it.

Charter: