

28 October 2008

By: Lucian Constantin, Web News Editor



Opera affected by  
0-day remote code  
execution vulnerability  
Opera Software ASA

## [Opera Zero Day Remote Code Execution Vulnerability](#)

*The latest stable version is vulnerable*

Opera 9.61 security update was released last week and fixed a vulnerability in the browser's History Search feature which allowed for remote attackers to read the browser history of the users visiting a maliciously crafted web page. Even though Opera rated this vulnerability as "Extremely Severe", it seems that they did not properly analyze the flawed resource, as security researchers have just announced a remote code execution vulnerability originating in the same code.

The new vulnerability was discovered when security researchers Roberto Suggi Liverani, Stefano Di Paola, and Aviv Raff took a closer look at the patched XSS history search vulnerability. Roberto Suggi Liverani, IT Security Consultant at Security Assessment, is also the researcher credited with discovering and reporting the original History Search flaw to Opera.

The remote code execution is more dangerous than the previous one as it allows for any potentially malicious code to be executed when a user visits a page set up by the attacker. Aviv Raff created a proof of concept exploit page that executes the calc.exe application on Windows machines when it is visited. Even though this example no longer works in 9.61, Raff claims that he has another PoC that does, but he will only release it after Opera fixes the issue. The researcher pointed out that the Linux and Mac OSX versions of Opera are also affected.

"They should have looked at the code of this local resource for more vulnerabilities. The fixed one is within the displayed links in the searched history. The unfixed one is within the Previous/Next links of the history search page itself," commented Aviv Raff for [The Register](#)

Opera has been notified about the new flaw and is currently working on a fix which will be included in the 9.62 update. According to Thomas Ford, spokesman for Opera Software, there is no exact release date for Opera 9.62, but he estimates that it will come very soon.

The Register reports that Mr. Ford also commented on the latest security issues discovered. "We always appreciate people digging and looking for security vulnerabilities in our products. We want them to be as robust as they can be," he stated.