Zero-day vulnerabilities in Firefox extensions discovered

Posted on 20 November 2009.

One of the reasons behind Firefox's popularity is the availability of a vast library of extensions. Users use them to modify the browser to their liking and make their browsing experience easier and more pleasant. The problem is, unbeknown to them, these extensions are exposing them to risk.

At the SecurityByte & OWASP AppSec Conference in India, Roberto Suggi Liverani and Nick Freeman, security consultants with security-assessment.com, offered insight into the substantial danger posed by Firefox extensions.

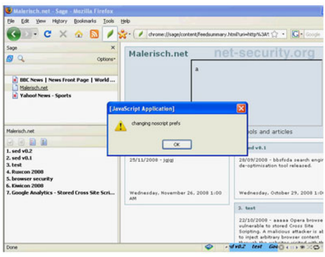
Mozilla doesn't have a security model for extensions and Firefox fully trusts the code of the extensions. There are no security boundaries between extensions and, to make things even worse, an extension can silently modify another extension.

Any Mozilla application with the extension system is vulnerable to same type of issues. Extensions vulnerabilities are platform independent, and can result in full system compromise.

The researchers believe that the weakest link in the chain is the human factor. Many add-on developers do it for a hobby and are not necessarily aware of how dangerous a vulnerable extension can be. The extension reviewers don't need to have great knowledge about Web application security and follow guidelines on finding malicious extensions. This means vulnerable extensions can easily slip through.

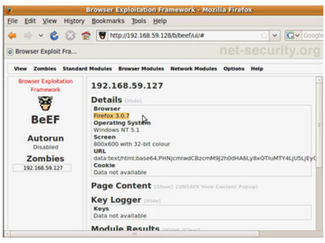
Researchers have found several bugs in popular Firefox extensions that have an estimate total amount of 30 million downloads from AMO (Addons Mozilla community site). Three 0days were also released at the SecurityByte & Owasp AppSec Asia 2009 conference.

Sage 1.4.3 and previous
HTML and JavaScript in the <description> tags of RSS feeds is executed in the chrome security zone. There is no filtering or protection.



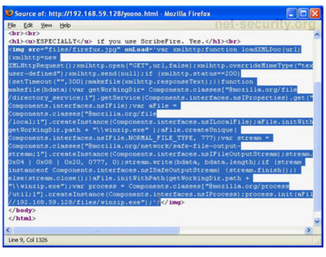
When you click on a malicious feed, it changes your NoScript settings and introduces the website in question on the whitelist of websites that are allowed to execute scripts.

InfoRSS 1.1.4.2 and previous
HTML and JavaScript in the <description> tags of RSS feeds is executed in the chrome security zone.



JavaScript is encoded in base64 or used as the source of an iframe and is executed automatically when the malicious feed items are scrolling in the status bar. At the same moment, remote attacker running BeEF (Browser Exploitation Framework) can start using the remote computer as its own zombie. By sending a set of remote commands, attacker gains full access to the computer.

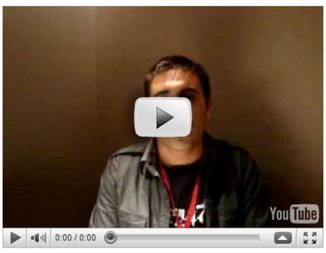
Yoono 6.1.0 and previous
JavaScript in DOM event handlers such as onLoad is evaluated in the chrome privileged browser zone.



Yoono is free software that allows you to connect and share with all your social networks and instant messaging services in one place. By using this extension, users can quickly save and share images from other web sites.

The problem here is that when using the extension on a malicious web site, remote file can be automatically downloaded and executed on your machine. Reverse VNC is just one of the options that can lead to the full compromise.

Speaking for Help Net Security, security researcher Roberto Suggi Liverani discusses his findings:



LATEST NEWS » Friday, 01:12 EDT

- Adobe releases Acrobat, Reader security updates
- Anonymizing anti-censorship tool for thwarting repressive regimes
- Justin Bieber offering free tickets on Facebook? It's a scam
- 40 Windows apps affected by critical code execution flaw
- Intel to acquire McAfee
- Top 10 most dangerous celebrity searches
- Oracle interrupted: Stealing sessions and credentials
- FGET: Network-capable forensic data acquisition tool
- New ICQ worm spreads like fire
- Twitter app demonstrates spammers have nothing to worry about
- Resourceful attackers continue to make the web insecure
- Employees admit they would steal data when leaving a job

More recent news

- Adobe releases Acrobat, Reader security updates
- Anonymizing anti-censorship tool for thwarting repressive regimes
- Justin Bieber offering free tickets on Facebook? It's a scam
- 40 Windows apps affected by critical code execution flaw
- Intel to acquire McAfee

Discover even more great content below:

NEWS | ARTICLES | REVIEWS | MALWARE CENTER