

Re: [Full-Disclosure] [Advisory] Mozilla Products Remote Crash Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-12/0214.html>

From: Heikki Toivonen (heikki_at_osafoundation.org)

Date: 12/07/04

To: bugtraq@securityfocus.com, full-disclosure@lists.netsys.com

Date: Mon, 06 Dec 2004 15:09:23 -0800

This crash was fixed today.

FYI – simple unexploitable crashes are generally not considered security issues by mozilla.org. With unexploitable crash I mean something that will only allow you to crash the product. An example of exploitable crash would be a buffer overflow, which often causes crash.

The reason for this is that simply crashing a client product is not that big of a deal, because it is easy to avoid. Crash on evil.com? Don't go there. If it is not easy to avoid, i.e. it is really a permanent DoS, then it will be dealt quickly as a security issue. (Yeah, I do know even a simple crash is annoying even if you know how to avoid it in the future. I'd be happy if someone went and fixed all the obscure crashers in Mozilla.)

Things are different for server products, and some parts of the Mozilla codebase are widely used in servers. In those cases any crash is considered a security issue. An example of such a component is the Network Security Services (NSS) which is used in web servers.

This does not mean crashes will be ignored and will go unfixed. It just means that they do not receive the urgency that exploitable crashes and other vulnerabilities receive.

As a security researcher, I would think it would be your responsibility to determine the seriousness of an issue. Just saying an app crashes does not make a security researcher IMO. Even my mom would be able to report a simple crash.

> *Niek van der Maas wrote:*

>> *I'm posting it here, the Mozilla guys didn't want to answer or even*

>> *confirm this bug. No idea whether this one is exploitable or not, I'll*

>> *leave that over to the readers of these lists.*

>> *DESCRIPTION*

>> *While working on one of my projects I discovered a vulnerability in*

Full-Disclosure: Re: [Full-Disclosure] [Advisory] Mozilla Products Remote Crash Vulnerability

>> *Firefox,*
>> *allowing a attacker to crash the browser. Further investigation*
>> *learned that*
>> *this vulnerability also applies on other Mozilla products, like*
>> *Navigator.*
>> *VENDOR RESPONSE*
>> *The bug (#272381) was opened 2004-11-30 in Bugzilla.*
>> *Until now (2004-12-06), no response or confirmation is received.*
>> *Contacting*
>> *the Mozilla Security Team on IRC didn't help either, it seems that*
>> *they're*
>> *simply not interested.*

--

Heikki Toivonen

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>

- application/pgp-signature attachment: OpenPGP digital signature