
Advisory:
Mozilla Firefox User Interface Null Pointer Dereference Dispatcher Crash and Remote Denial of Service.

Version Affected:
Mozilla 3.0.3 - 1.9.0 Branch (Specifically for Latest Version)

Release Date:
Disclosed: 28 September 2008
Release Date. 28 September ,2008

Description:
The mozilla firefox is vulnerable to user interface event dispatcher null pointer dereference denial of service attacks. The dispatched event created dynamically leads to firefox crash when it is called directly or in a defined loop with number of generated user interface events.The resultant crash results in

Exception Type: EXC_BAD_ACCESS (SIGBUS)
Exception Codes: KERN_PROTECTION_FAILURE at 0x0000000000000007
Crashed Thread: 0
Thread 0 Crashed: 0 libxpcom_core.dylib nsTArray_base::Length() const + 11 (nsTArray.h:66)
1 libgklayout.dylib nsContentUtils::GetAccelKeyCandidates(nsIDOMEvent*, nsTArray&) + 261 (nsContentUtils.cpp:4083)

This security issue is a result of unhandled exception which is a result of null pointer dereference.

Proof-of-Concept:
Click Here

Credit:
Aditya K Sood (Founder, www.Secniche.org)
Team Lead, www.EvilFingers.com

Disclaimer
