Advisory : Internet Explorer Zone Domain Specification Dos and Page Suppressing

Severity : Intermediate

Version : IE 6.0 - 7.0

CVE : 2007-3550

BID : 24744

Dated : 18 June 2007

By: Aditya K Sood [www.secniche.org]

Explanation:
The vulnerability is present in handling of domain names with different parameters [sub domains] when specified in the Intranet zone and Restricted zone with different characters [* ,.]. The Internet Explorer show weird behavior in opening of those websites. The problem occurs in loading of those websites there by resulting in DoS through the browser. The problem occurs in resolving domain names in different zones by the explorer. It can be launched remotely by a malicious attacker by exploiting this vulnerable behavior through a rogue script and registry functions. The problem persists if rogue entries or manipulated entries are subjected into various zones. The domain entries are specified in the registry with Zone numbers as defined below.

The Internet settings are properly addressed directly with registry. There is ZoneMap and Zone is defined as proper registry sub keys. If one look at the registry then a numeric value is given to the various zones ie 1,2,3,4 . In this a specified folder of desired domain is always present. In the folder www protocol is specified and DWORD value has to be provided with the Zone value [1,2,3,4]. The value define the domain to be present in a specific zone. An attacker can design a malicious script in Javascript in which a number of domain and sub domain entries are defined with meta characters for filling up a zone. It results in Denial of Service Attack when ever a user visit an untrusted website, after the inclusion of that script. The main point of an attacker is to fill the zone with crafted domain names so that core service failure occurs

So when a new instance of IE is loaded , the registry entries are triggered up there by resulting in security impacts. The website page gets suppressed. The page gets hanged for sometime , there by showing a delay in loading of website and affects the CPU load.

Vendor Status : Reported To Microsoft Security Center.

Solution By Microsoft Security Center:

1. Avoid visiting untrusted Websites.
2. Script Restriction should be applied.

External Links:
http://www.securityfocus.com/bid/24744
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3550
http://nvd.nist.gov/cpe.cfm?cvename=CVE-2007-3550