
Advisory: Google Chrome FTP PASV IP Malicious Scanning Vulnerability.

Version Affected: Google Chrome: 1.0.154.36

Release Date:
Disclosed: 1 January 2009
Released: 4 January 2009

Description:
Google Chrome FTP Client is vulnerable to FTP PASV malicious port scanning vulnerability.The username in the FTP (ftp://username:password@domain.com) can be manipulated by tampering it with certain IP address with specification of port as (ftp://xxx.xxx.xxx.xxx-22:password@domain.com).The Google Chrome FTP client make connection to the rogue FTP server which uses PASV commands to scan network.Dynamic requests are issued to a rogue FTP server which accepts connection with different usernames as the IP address with specified ports to locate the non existing object on the target domain. JavaScript Port Scanning is used to exploit this issue. A malicious web page hosted on a specially-coded FTP server could use this feature to perform a generic port-scan of machines inside the firewall of the victim.The generated fraudulent request helps attacker to exhibit internal network information through sustainable port scanning through JavaScript.

Proof-of-Concept:
Click Here
Alternate Link: http://www.secniche.org/gcfpv/

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

Disclaimer:
The information in the advisory is believed to be accurate at the time of publishing based on currently available information. Use of the information constitutes acceptance for use in an AS IS condition. There is no representation or warranties, either express or implied by or with respect to anything in this document, and shall not be liable for a ny implied warranties of merchantability or fitness for a particular purpose or for any indirect special or consequential damages.
