

NIPC ADVISORY 00-046

"FireWall-1 Vulnerability"

June 07, 2000

A number of reliable reports indicate FireWall-1 installations may be susceptible to Denial-of-Service attacks from incomplete or illegal data packet fragments. Software scripts already in existence are known to be capable of exploiting this vulnerability. It should be emphasized that the impact would be limited to Denial-of-Service, and no penetration through the firewall is involved.

Vendor testing has confirmed that product versions 4.0 and 4.1 are vulnerable. The vendor has provided an interim workaround until a more permanent solution is available. The workaround is available at the following web site:

[http:// www.checkpoint.com/techsupport/alerts/ipfrag_dos.html](http://www.checkpoint.com/techsupport/alerts/ipfrag_dos.html)

Recipients are asked to report significant or suspected criminal activity to their local FBI office or the NIPC Watch and Warning Unit, and to computer emergency response support and other law enforcement agencies, as appropriate. The NIPC Watch and Warning Unit can be reached at (202) 323-3204/3205/3206, or nipc.watch@fbi.gov.