

# Department of Homeland Security

## National Infrastructure Protection Center "Snort buffer overflow Vulnerability" Advisory 03-003

March 3, 2003

The Department of Homeland Security (DHS), National Infrastructure Protection Center (NIPC) has been informed of a recently discovered serious vulnerability in Snort, a widely used Intrusion Detection System, IDS. DHS/NIPC has been working closely with the Internet security industry on vulnerability awareness and is issuing this advisory in conjunction with public announcements.

Snort is available in open source and commercial versions from Sourcefire, a privately held company headquartered in Columbia, MD. Details are available from Sourcefire. See Snort Vulnerability Advisory [SNORT-2003-001]. The affected Snort versions include all version of Snort from version 1.8 through current. Snort 1.9.1 has been released to resolve this issue.

The vulnerability was discovered by Internet Security Systems (ISS), and is a buffer overflow in the Snort Remote Procedure Call, RPC, normalization routines. This buffer overflow can cause snort to execute arbitrary code embedded within sniffed network packets. Depending upon the particular implementation of Snort this may give local and remote users almost complete control of a vulnerable machine. The vulnerability is enabled by default. Mitigation instructions for immediate protections prior to installing patches or upgrading are described in the Snort Vulnerability Advisory.

Due to the seriousness of this vulnerability, the DHS/NIPC strongly recommends that system administrators or security managers who employ Snort take this opportunity to review their security procedures and patch or upgrade software with known vulnerabilities.

Sourcefire has acquired additional bandwidth and hosting to aid users wishing to upgrade their Snort implementation. Future information can be found at:  
<http://www.sourcefire.com/>

As always, computer users are advised to keep their anti-virus and systems software current by checking their vendor's web sites frequently for new updates and to check for alerts put out by the DHS/NIPC, CERT/CC, ISS and other cognizant organizations. The DHS/NIPC encourages recipients of this advisory to report computer intrusions to their local FBI office (<http://www.fbi.gov/contact/fo/fo.htm>) and other appropriate authorities. Recipients may report incidents online to <http://www.nipc.gov/incident/cirr.htm>. The DHS/NIPC Watch and Warning Unit can be reached at (202) 323-3204/3205/3206 or [nipc.watch@fbi.gov](mailto:nipc.watch@fbi.gov).