# CVE Detail – CVE-2010-0013

Directory traversal vulnerability in slp.c in the MSN protocol plugin in libpurple in Pidgin 2.6.4 and Adium 1.3.8 allows remote attackers to read arbitrary files via a .. (dot dot) in an application/x-msnmsgrp2p MSN emoticon (aka custom smiley) request, a related issue to CVE-2004-0122. NOTE: it could be argued that this is resultant from a vulnerability in which an emoticon download request is processed even without a preceding text/x-mms-emoticon message that announced availability of the emoticon.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.93552

## CVSS Scoring

CVSS v3.1 Score: 7.5

Severity: HIGH

## Mapped CWE(s)

* CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

## CAPEC(s)

* CAPEC-126: Path Traversal
* CAPEC-64: Using Slashes and URL Encoding Combined to Bypass Validation Logic
* CAPEC-76: Manipulating Web Input to File System Calls
* CAPEC-78: Using Escaped Slashes in Alternate Encoding
* CAPEC-79: Using Slashes in Alternate Encoding

## Affected Products

* cpe:2.3:a:adium:adium:1.3.8:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:pidgin:pidgin:2.6.4:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:11:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:12:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:opensuse:opensuse:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:linux\_enterprise:11.0:-:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:linux\_enterprise\_server:10:sp2:\*:\*:-:\*:\*:\*
* cpe:2.3:o:suse:linux\_enterprise\_server:10:sp3:\*:\*:-:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux:4.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux:5.0:\*:\*:\*:\*:\*:\*:\*