

# [UNIX] ike-scan Buffer Overflow Vulnerabilities

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-06/0082.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 06/24/03

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 24 Jun 2003 16:15:53 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

Beyond Security in Canada

Toronto-based Sunrays Technologies is now Beyond Security's representative in Canada.

We welcome ISPs, system integrators and IT systems resellers

to promote the most advanced vulnerability assessment solutions today.

Contact us at 416-482-0038 or at [canadasales@beyondsecurity.com](mailto:canadasales@beyondsecurity.com)

-----

ike-scan Buffer Overflow Vulnerabilities

---

## SUMMARY

<<http://www.nta-monitor.com/ike-scan/>> ike-scan, a VPN Discovery and Fingerprinting tool, has been found to contain a buffer overflow vulnerability.

## DETAILS

Vulnerable code:

Vulnerable code can be found in ike-scan.c:295

.....

```
for (arg=0; arg<argc; arg++) {
    strcat(arg_str, argv[arg]);
    if (arg < (argc-1)) {
        strcat(arg_str, " ");
    }
}
```

.....

Example:



Securiteam: [UNIX] ike-scan Buffer Overflow Vulnerabilities

```
(gdb) x/i $eax
0x41414141: Cannot access memory at address 0x41414141
(gdb) x/i 0x08048da2
0x8048da2 <main+126>: pushl (%eax,%ebx,4)
(gdb)
```

ponit:argv=0x41414141 ,problem in \*argv(),

ADDITIONAL INFORMATION

The information has been provided by <mailto:jsk@ph4nt0m.net> jsk.

=====

This bulletin is sent to members of the SecuriTeam mailing list.  
To unsubscribe from the list, send mail with an empty subject line and body to:  
list-unsubscribe@securiteam.com  
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====  
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.  
In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.