
Suresec security advisory 5
16 th August 2005
CVE IDs: CAN-2005-2514, CAN-2005-2521, CAN-2005-2508

# Buffer overflow in ping and traceroute.

**Vulnerability summary:**
The ping and traceroute programs used in Mac OS X are vulnerable to a buffer overflow when resolving a hostname. In the case of ping a hostname gets copied into a static buffer which is 80 bytes long. For traceroute the hostname gets copied into a static buffer which is 50 bytes long as shown by the following code snippets:
ping:

```
char * pr_addr(u_long l) {
        struct hostent *hp;
        static char buf[80];

        if ((options & F_NUMERIC) ||
            !(hp = gethostbyaddr((char *)&l, 4, AF_INET)))
                (void)sprintf(buf, "%s", inet_ntoa(*(struct in_addr *)&l));
        else
                (void)sprintf(buf, "%s (%s)", hp->h_name,
                    inet_ntoa(*(struct in_addr *)&l));
        return(buf);
}
```

traceroute:

```
char * inetname(struct in_addr in) {
        register char *cp;
        static char line[50];
        struct hostent *hp;
        static int first = 1;
       ...
        if (first && !nflag) {
                first = 0;
             ...
       }
        cp = 0;
        if (!nflag && in.s_addr != INADDR_ANY) {
                hp = gethostbyaddr((char *)&in, sizeof (in), AF_INET);
                if (hp) {
                    ...
                        cp = hp->h_name;
                }
        }
        if (cp)
                (void) strcpy(line, cp);
       ...
```

**Impact:**
When properly exploited this yields local root.

**Affected versions:**
all versions of Mac OS X up to 10.3.9 and 10.4.2 are affected.

**Suggested Recommendations:**
apply the apple security updates.

**Credits:**
Ilja van Sprundel found these vulnerabilities.

# User spoofing vulnerability in dsidentity.

**Vulnerability summary:**
dsidentity is a tool to add or remove users. For specific actions it is required that the user is in the admin group. The code being used to validate if a user is in the admin group or not uses getenv, as shown by the following code snippet:

```
char *envStr = nil;
envStr = getenv("USER");
//check for member of admin group
if ( (envStr != nil) && UserIsMemberOfGroup( inDSRef, inDSNodeRef, envStr,
"admin" ) )
{
	return true;
}
```

**Impact:**
When properly exploited users can remove any user account.

**Affected versions:**
all versions of Mac OS X 10.4.x up to 10.4.2 are affected.

**Suggested Recommendations:**
apply the apple security updates.

**Credits:**
Neil Archibald found this vulnerability.

**About us:**
Suresec Ltd is a global service provider of Internet security solutions and consultancy with unmatched quality from our world class consultancy practice.

Our consultants have pioneered in the field of security research and have closely worked with leading software companies and service providers to mitigate risks and fix a number of critical vulnerabilities, Suresec also works closely with a number of open source companies to provide them with a source code auditing and technical consultancy. We have a strong team consultants spread across Europe, the United States of America And Australia specializing in security consulting.