



**sureSEC**  
SECURING THE SOURCE

Suresec security advisory 8  
3<sup>th</sup> November 2005  
CVE ID: CVE-2005-1126, CVE-2005-2752

# Mac OS X kernel (xnu) multiple information leaks.

## Vulnerability summary:

The first information leak found in xnu is located in the ifconf() function (used to retrieve information about all used network interfaces). The leak exists because a buffer that will contain a string does not get initialized first. When the buffer is copied back to the user there will usually be about 12 bytes of uninitialized memory leaked to the user, as shown by the following code snippet:

```
ifconf(cmd, data)
    u_long cmd;
    caddr_t data;
{
    register struct ifconf *ifc = (struct ifconf *)data;
    register struct ifnet *ifp = ifnet.tqh_first;
    register struct ifaddr *ifa;
    struct ifreq ifr, *ifrp;
    ...
    ifrp = ifc->ifc_req;
    for (;space >sizeof (ifr) && ifp; ifp = ifp->if_link.tqe_next) {
        char workbuf[64];
        ...
        ifnlen = snprintf(workbuf, sizeof(workbuf), "%s%d",
            ifp->if_name, ifp->if_unit);
        ...
        strcpy(ifr.ifr_name, workbuf);
        ...
        error = copyout((caddr_t)&ifr, (caddr_t)ifrp, sizeof (ifr));
        ....
    }
    ...
}
```

## Impact:

When properly exploited this can lead to kernel memory being disclosed to a user process. Such memory might contain sensitive information, such as portions of the file cache or terminal buffers. This information might be directly useful, or it might be leveraged to obtain elevated privileges in some way. For example, a terminal buffer might include a user-entered password.

## Affected versions:

This vulnerability affects all 10.3.x and 10.4.x versions of Mac OS X. Because of the shared code base with FreeBSD this vulnerability was also present in all versions of FreeBSD Up until 5.4-RELEASE.

**Suggested Recommendations:**

There is a security update for OS X 10.4.x (See Mac OS X 10.4.3 Update) It is advised that you make use if this update. We are currently unaware of and security upgrade for OS X 10.3.x. For FreeBSD see FreeBSD-SA-05:04.ifconf.

**Credits:**

Ilja van Sprundel found this vulnerability.

### **Vulnerability summary:**

The second information leak found in xnu is located in the `atp_pack_bdsp()` function (used for appletalk communication). The leak exists because of a signedness problem. It is possible to specify a short negative value to be copied back to userland. This allows a potential attacker to bypass a boundcheck done and then allows leaking of an almost arbitrary amount of kernel memory as shown by the following code snippet:

```
static void
atp_pack_bdsp(trp, bdsp)
    register struct atp_trans *trp;
    register struct atpBDS *bdsp;
{
    register gbuf_t *m = NULL;
    register int i, datsize = 0;
    struct atpBDS *bdsbase = bdsp;

    dPrintf(D_M_ATP, D_L_INFO, ("atp_pack_bdsp: socket=%d\n",
        trp->tr_queue->atp_socket_no));

    for (i = 0; i < ATP_TRESP_MAX; i++, bdsp++) {
        short bufsize = UAS_VALUE(bdsp->bdsBuffSz);
        ...
        while (m) {
            short len = (short)(gbuf_len(m));
            if (len) {
                if (len > bufsize)
                    len = bufsize;
                copyout((caddr_t)gbuf_rptr(m),
                    (caddr_t)&buf[tmp],
                    len);
                bufsize -= len;
                tmp += len;
            }
            m = gbuf_cont(m);
        }
        ...
    }
}
```

### **Impact:**

When properly exploited this can lead to kernel memory being disclosed to a user process. Such memory might contain sensitive information, such as portions of the file cache or terminal buffers. This information might be directly useful, or it might be leveraged to obtain elevated privileges in some way. For example, a terminal buffer might include a user-entered password.

### **Affected versions:**

This vulnerability affects all 10.3.x and 10.4.x versions of Mac OS X.

**Suggested Recommendations:**

There is a security update for OS X 10.4.x (See Mac OS X 10.4.3 Update) It is advised that you make use of this update. We are currently unaware of and security upgrade for OS X 10.3.x.

**Credits:**

Ilja van Sprundel 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 of consultants spread across Europe, the United States of America and Australia specializing in security consulting.