suresec
SECURING THE SOURCE

Suresec security advisory 1
Release date: 27th March 2005
CVE ID: CAN-2005-0750

Linux kernel local root vulnerability

About the linux kernel:
The linux kernel is a widely used kernel which is unix based.

Vulnerability summary:
The linux kernel has support for bluetooth. A local root security vulnerability was found in this bluetooth stack.
Vulnerable code:

```
static int bluez_sock_create(struct socket *sock, int proto)
{
        if (proto >= BLUEZ_MAX_PROTO)
                return -EINVAL;
        ...
        return bluez_proto[proto]->create(sock, proto);
}
```

This code can be reached by either calling socket() or alternativly calling socketpair(). When passed a negative value for the protocol the bounds check can be bypassed. Later the protocol number is used as an index to a function pointer. It is possible to use proto as an index to some kind of memory that is under a user's control.

Impact:
When properly exploited this yields local root. (exploitation is trivial)

Affected versions:
This vulnerability affects all 2.6.x(.y) <= 2.6.11.5 linux kernels and >= 2.4.6 <= 2.4.30-rc1kernels provided that there is support for bluetooth.

Suggested Recommendations:
Update your kernel to a newer one, or alternativly we've made a loadable kernel modules which works around the problem by checking the protocol and domain before the bluetooth socket code is called. It can be found at:
http://www.suresec.org/tools/bluetooth_workaround.tar.gz

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 consultants spread across Europe, the United States and Australia specializing in security consulting.