Suresec security advisory 2
9th May 2005
CVE ID: CAN-2005-1461

Remote root vulnerability in Ethereal.

About ethereal:
Ethereal is a widely used network packet capturing utility which has support for over 700 network protocols.

Vulnerability summary:
Ethereal has a dissector for the distcc network protocol. A stack based bufferoverflow was discovered in parsing argv, serr and sout messages.
Vulnerable code:

```
static void dissect_distcc(tvbuff_t *tvb, packet_info *pinfo, proto_tree
*parent_tree)
{
        char token[4];
        guint32 parameter;

        while(1){
             tvb_memcpy(tvb, token, offset, 4);
             ...
             sscanf(tvb_get_ptr(tvb, offset, 8), "%08x", &parameter);
             ...
             } else if(!strncmp(token, "ARGV", 4)){
                offset=dissect_distcc_argv(tvb, pinfo, tree, offset, parameter);
             }
             ...
        }
}

static int dissect_distcc_argv(tvbuff_t *tvb, packet_info *pinfo _U_,
                        proto_tree *tree, int offset, gint parameter)
{
        char argv[256];
        int argv_len;
        gint len=parameter;
        argv_len=len>255?255:len;
        tvb_memcpy(tvb, argv, offset, argv_len);
        ...
}
```

When given a negative value for parameter the bounds check will be bypassed and an overflow in memcpy occurs.

Impact:
When properly exploited this yields remote root.

Affected versions:
This vulnerability affects Ethereal version 0.9.13 up untill 0.10.10.

Suggested Recommendations:
Turn off support for distcc or update to a newer version of ethereal.

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 of America And Australia specializing in security consulting.