

[NT] DameWare Passes Weak File Encryption Key in the Clear

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-03/0071.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 03/25/04

To: list@securiteam.com

Date: 25 Mar 2004 16:45:04 +0200

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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

DameWare Passes Weak File Encryption Key in the Clear

SUMMARY

<<http://www.dameware.com/>> DameWare Mini Remote, "A lightweight remote control intended primarily for administrators and help desks for quick and easy deployment without external dependencies and machine reboot". DameWare Mini Remote has been found to contain a vulnerability that would allow an attacker to hijack content sent by DameWare supposedly in a secure manner (encrypted).

DETAILS

Vulnerable Systems:

* DameWare Mini Remote Control version 4.1.0.0 and prior

DameWare Mini Remote Control passes a Blowfish encryption key over the wire in the clear. It is bad enough that they appear to be using Blowfish in Electronic Codebook Mode; but they compound their errors by the following two vulnerabilities:

1) The DameWare Mini Remote Control offers the capability to transfer files between the host and client encrypted using 128-bit Blowfish

Securiteam: [NT] DameWare Passes Weak File Encryption Key in the Clear

Encryption. Their first mistake is using a poor random bit generator to create their encryption key. After identifying the key in the clear I was able to surmise that the lack of cryptographic expertise of the DameWare developers was systemic and checked to see if they were using the built-in rand() function to generate the key. It did not take long to exhaust the small space of the Windows' linear congruential generator (LCG) in rand() to discover the following hypothesized loop for generating their file encryption key.

```
int i;
unsigned char dw_f_key[16];
srand(time(NULL));
for(i=0;i<16;i++){
    dw_f_key[i] = rand();
}
```

2) A more serious mistake is that they actually pass the file encryption key in the clear over the wire. This can be seen by analyzing packets between host and target. In a packet just prior to the file being sent the second to the last string of 16-bytes is the file encryption key.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:ax09001h@hotmail.com>>
ax09001h.

=====

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.