

[NEWS] Weak Password Encryption Scheme in Integrated Dialer Software for VSNL

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-11/0005.html>

From: support@securiteam.com

Date: 11/03/02

From: support@securiteam.com

To: list@securiteam.com

Date: 3 Nov 2002 14:18:59 +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

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.

Weak Password Encryption Scheme in Integrated Dialer Software for VSNL

SUMMARY

VSNL is one of India's largest Internet Service Providers. It provides its subscribers with an Integrated Dialer, which is a sort of replacement to Windows Dial-up Networking. This Dialer is available for free download from its website <<http://internet.vsnl.net.in/dialer/vsnlsetup.exe>> <http://internet.vsnl.net.in/dialer/vsnlsetup.exe>. The (dis)advantage of the Integrated Dialer is that it shows streaming ads while the user is surfing.

The Integrated Dialer comes with the option where-in the user can check the option "Save Password", so that he need not enter the password again. However, the algorithm used to encrypt and store the password is very weak and can be easily decrypted as shown below.

DETAILS

Vulnerable systems:

* Integrated Dialer Software for VSNL version 1.2.000

Impact:

The weakly encrypted password is one which is used by users to connect to VSNL for Internet access, as well as to authenticate to their email

Securiteam: [NEWS] Weak Password Encryption Scheme in Integrated Dialer Software for VSNL

account. Any compromise of this password would mean their Internet account being stolen as well as their emails being compromised. However, to decrypt the password, local registry access would be required.

Details:

The encryption algorithm uses a simple one-to-one mapping technique which can easily be deciphered. The encrypted password is stored in the follow registry key, which is constant on all windows platforms:

Hive: HKEY_LOCAL_MACHINE\SOFTWARE

Key : \VSNL.COM\Dialer\Config

Name: Password

Type: REG_SZ

The array used to map the password-to-encrypted data is given below:

abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ`~!@#4\$5%6^7&8*9(0)-_+=+[{]};:','<.>

During encryption, the above characters are mapped one-to-one with the below array.

~!@#%\$^&*()_+1234567890-=[{]};:','<.>/?aAbBcCdDeEfFgGhHiIjJkKlLmMnNoOpPqQrRsStTuUvVwWxXyYzZ

For decryption, a simple reverse mapping is carried out.

PoC Decryption Utility:

Arjun has coded a simple utility in Assembly code to demonstrate the encryption / decryption routine. You can download it along with the source code from <<http://www.nii.co.in/vuln/idvsnl.html>>
<http://www.nii.co.in/vuln/idvsnl.html>.

Vendor Response and Timeline:

21 Oct 2002: Email sent to vendor about the vulnerability

28 Oct 2002: Reminder email sent as per our Vulnerability Disclosure Policy (<<http://www.nii.co.in/vdp.html>> <http://www.nii.co.in/vdp.html>)

1st Nov 2002: Advisory posted. Arjun decided to go ahead and post this advisory, since no vendor response was forthcoming even after repeated emails.

Workarounds:

Do not use the Save As option in the Dialer. If you were using that option earlier, delete the registry key mentioned above. Better still use good old DUN instead.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:arjunp@nii.co.in>> Arjun Pednekar.

=====

Securiteam: [NEWS] Weak Password Encryption Scheme in Integrated Dialer Software for VSNL

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: "[\[NEWS\] NetScreen SSH1 CRC32 Denial of Service](#)"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)