

[NT] Prevx Pro Multiple Vulnerabilities (File Protection Bypass, Command Bypass)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-08/0015.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/02/05

To: list@securiteam.com

Date: 2 Aug 2005 18:07:36 +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>

Prevx Pro Multiple Vulnerabilities (File Protection Bypass, Command Bypass)

SUMMARY

" <<http://www.prevx.com/>> Prevx Pro utilizes the latest behavior based intrusion prevention technology." By using memory mapping it is possible to access the programs that Prevx protects. In addition, by sending invalid information it is possible to tell Prevx to allow a malicious program to penetrate the system.

DETAILS

Vulnerable Systems:

* Prevx Pro IPS 2005

File Protection Bypass:

Prevx by default protected many critical files of the system. However, the protection can be bypassed by using memory mapping. For example, to edit winnt/win.ini file, open the file and do mapviewoffile, and then edit the file from the memory. Prevx does not protect files being edited from memory mapping IO.

Securiteam: [NT] PrevX Pro Multiple Vulnerabilities (File Protection Bypass, Command Bypass)

Command Bypass:

PrevX kernel driver and the user-space applications talking with each other by using NtDeviceIoControlFile. However, it seems the driver doesn't check whether or not the user-application is from PrevX or not. It is possible to bypass the protection by pretending a user send an "allow" command down to the kernel driver every time a warning message is popping up.

ADDITIONAL INFORMATION

The information has been provided by <mailto:trihuynh@huynhsec.com> Tri Huynh.

=====

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.