

[NT] NGSEC StackDefender 2.0 Invalid Pointer Dereference Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-08/0030.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/10/04

To: list@securiteam.com

Date: 10 Aug 2004 19:14:46 +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>

NGSEC StackDefender 2.0 Invalid Pointer Dereference Vulnerability

SUMMARY

StackDefender is "an IPS (Intrusion Prevention System), for Win32 platforms, that will deny shellcode from executing in User Stack and Writeable memory regions. StackDefender uses PAX technology for this purpose". A vulnerability exists because StackDefender fails to verify 'BaseAddress' as a valid address prior dereferencing it as a pointer.

DETAILS

Vulnerable Systems:

- * StackDefender version 2.0

Immune Systems:

- * StackDefender version 2.10

StackDefender offers protection by hooking ZwAllocateVirtualMemory and ZwProtectVirtualMemory functions. These two kernel API's are responsible for allocating and protecting memory. The ZwProtectVirtualMemory function declaration is as follows:

```
ZwProtectVirtualMemory(HANDLE ProcessHandle, PVOID *BaseAddress,
```

Securiteam: [NT] NGSEC StackDefender 2.0 Invalid Pointer Dereference Vulnerability

PULONG ProtectSize, ULONG NewProtect, PULONG OldProtect);

The problem specifically exists because StackDefender fails to verify 'BaseAddress' as a valid address prior dereferencing it as a pointer.

Analysis:

Successful exploitation allows remote attackers to cause the underlying system to crash. This is possible by specifying an invalid address for 'BaseAddress'. Exploitation requires that an attacker has an exploitation vector to the system that StackDefender attempts to block.

Vendor Fix:

The vendor has released the following patch fixing this issue:

<<http://www.ngsec.com/downloads/stackdefender/StackDefender-2.10.exe>>
<http://www.ngsec.com/downloads/stackdefender/StackDefender-2.10.exe>

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0766>>
CAN-2004-0766

Disclosure Timeline:

- 07/10/2004 Vulnerability discovered by iDEFENSE
- 07/12/2004 Initial vendor notification
- 07/22/2004 Initial vendor response
- 08/03/2004 Public disclosure

ADDITIONAL INFORMATION

The information has been provided by
<<mailto:idlabs-advisories@idefense.com>> iDEFENSE.

The original article can be found at:
<<http://www.idefense.com/application/poi/display?id=119&type=vulnerabilities&flashstatus=true>>
<http://www.idefense.com/application/poi/display?id=119&type=vulnerabilities&flashstatus=true>

=====

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.