

[NT] ZoneAlarm Invalid Pointer Dereference Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-02/0042.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 02/13/05

To: list@securiteam.com

Date: 13 Feb 2005 13:15:19 +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>

ZoneAlarm Invalid Pointer Dereference Vulnerability

SUMMARY

<<http://www.zonelabs.com/>> Zone Labs ZoneAlarm "provides personal firewall protection". Local exploitation of an invalid pointer dereference vulnerability in Zone Labs LLC's ZoneAlarm personal firewall allows attackers to trigger a denial of service (DoS) condition.

DETAILS

Vulnerable Systems:

- * ZoneAlarm version 5.1 and prior

Immune Systems:

- * ZoneAlarm version 5.5 or newer

ZoneAlarm offers process specific protection by hooking the kernel API routine NtConnectPort(). NtConnectPort() is used by programs to implement advanced inter-process communication (IPC). The NtConnectPort() function is declared as follows:

```
NtConnectPort(
    OUT PHANDLE ClientPortHandle,
```

Securiteam: [NT] ZoneAlarm Invalid Pointer Dereference Vulnerability

```
IN PUNICODE_STRING ServerPortName,  
IN PSECURITY_QUALITY_OF_SERVICE SecurityQos,  
IN OUT PLPC_SECTION_OWNER_MEMORY ClientSharedMemory OPTIONAL,  
OUT PLPC_SECTION_MEMORY ServerSharedMemory OPTIONAL,  
OUT PULONG MaximumMessageLength OPTIONAL,  
IN OUT PVOID ConnectionInfo OPTIONAL,  
IN OUT PULONG ConnectionInfoLength OPTIONAL);
```

The problem specifically exists within vsdatant.sys as ZoneAlarm fails to verify the second argument. 'ServerPortName' is a valid address prior to dereferencing it as a pointer. The vulnerable section of code is displayed here:

```
0001EE93 mov esi, [esp+108h+ServerPortName]  
0001EE9A mov edi, eax  
0001EE9C test esi, esi  
0001EE9E jz short loc_1EEB6  
0001EEA0 mov edx, [esi+4]
```

The argument 'ServerPortName' is stored in the register ESI. A check is made to ensure that the value is not NULL. If that check is passed, the value is dereferenced as a pointer. Any non-zero invalid memory address can be passed as the second argument to NtConnectPort(), resulting in a system crash.

Analysis:

Exploitation allows local and remote attackers who have exploited another vulnerability to trigger a DoS in kernel space, resulting in a "blue screen of death."

Vendor response:

A vendor advisory for this issue is available at:

<http://download.zonelabs.com/bin/free/securityAlert/19.html>

<http://download.zonelabs.com/bin/free/securityAlert/19.html>

CVE Information:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0114>

CAN-2005-0114

Disclosure Timeline:

01/06/2005 – Initial vendor notification

01/07/2005 – Initial vendor response

02/11/2005 – Coordinated 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=199&type=vulnerabilities>

<http://www.idefense.com/application/poi/display?id=199&type=vulnerabilities>

Securiteam: [NT] ZoneAlarm Invalid Pointer Dereference Vulnerability

=====

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.