

RSUPPORT RemoteCall

Security white paper

Make IT Easy with RSUPPORT

RSUPPORT is proud of releasing 2009 New line of Products meeting growing needs of Remote Support market..

RemoteHelp – is a virtual help desk over the Internet and is able to have general representatives and professional representatives separately to increase the efficiency for large call centers and is a tool that contains automated distribution and queue system as a Advanced Remote Support **RemoteCall 5.0** – is a remote support tool that anyone from regular users to professionals can communicate each other easily via their browser.

RemoteSales – is a online-sales tool that enables sales professionals to make online presentation to customers anytime anywhere with reducing travel time and cost.

<http://www.rsupport.com>

Please visit RSUPPORT homepage for more information.

Go Secure with RSUPPORT

Introduction

RSUPPORT's products are remote support tools that anyone from regular users to professionals can give and get support easily with connecting each other via their browser.

RSUPPORT's products provide secured remote support in terms of the security vulnerability stated below that Web service might have.

Is ActiveX Vulnerable?

ActiveX has announced in the beginning of 1996, known as an extension version of COM (Component Object Model), It is now being integrated into .NET strategy these days through DCOM (Distributed COM). Actually, It seems that ActiveX has been announced as an alternative of SUN's JAVA. OLE (Object Linking and Embedding) technology which could be called Microsoft's revolution of API then, means the Objects linked with OLE could be applicable and executable to the other application.

ActiveX is based on the trust model. MS takes the method to permit the signed ActiveX Control, not for unsigned ActiveX. It is available when Signed ActiveX doesn't contain a malicious code in it.

Known security vulnerability is as below for ActiveX Controls.

1. Provide with Methods directly that can access to local resources
2. Malicious behavior using Update that distributes unintended files
3. Bypass the logic with the sophisticated forged input value
4. Malicious behavior that uses buffer overflow for the input value such as Method or Property
5. Malicious behavior that inserts malicious code(Black ActiveX) through the vulnerability of MS Website, requires everyone who visits the site to install it in Internet Explorer to be exposed to vulnerability, steal the private information from the infected PC and runs malicious system command.

ActiveX control could be executed by hackers to attack any one through web interface.

Image 1 Calls using Object Tag and Script

```
<OBJECT ID="update" WIDTH=0 HEIGHT=0 CLASSID="CLSID:3E01A824-">
<PARAM NAME="nam" VALUE='12'>
</OBJECT>

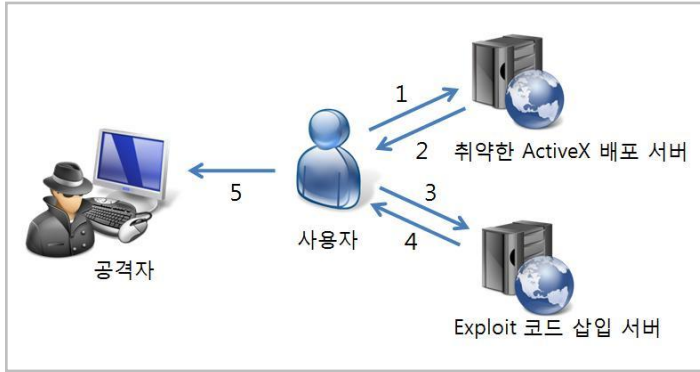
<script>

Update.Startupupdate()

</script>
```

As Active X vulnerability keeps being reported, A lot of exploit codes are open to the public. There are lots of simple Exploit code that Anyone can use easily among these.

Image 2 Hacking using ActiveX vulnerability



1. A User accesses a vulnerable Active X to use services as Banking, Game etc.
2. A User uses the service with installing the vulnerable ActiveX
3. A User accesses a website or bulletin board that has XSS vulnerability.
4. A malicious script Exploit code inserted is executed on the computer through XSS vulnerability
5. An attacker can control the resources of remote computer because local privilege of the user's computer is given to Attacker

You are required to install ActiveX control for most of website these days. It is being used in Online game installation program, Movie/Music player, Public certificates, Security programs(Key logger, Hacking protection, Online vaccine, PC Firewall, Spyware etc. Most of korean websites use ActiveX controls. RemoteCall 5 protects against ActiveX vulnerability with providing non-ActiveX Remote Support. RSUPPORT used to provide ActiveX remote support for RemoteCall v4.0. RSUPPORT doesn't insert any malicious code and use Parameters for arbitrary calling using Object Tag and Script and These parameters is encrypted to protect security vulnerability.

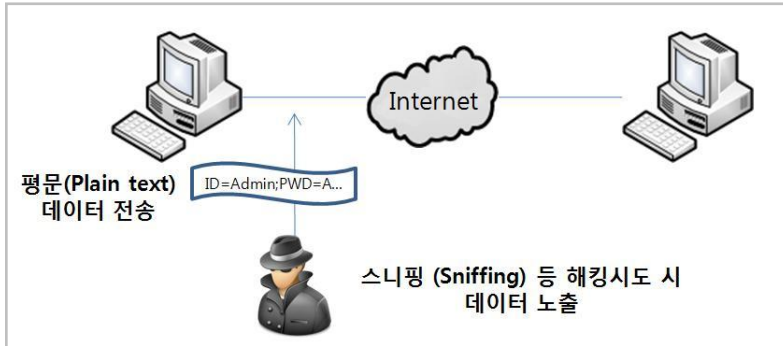
The sites run by RSUPPORT is running with analyzing and patching the vulnerability, also RSUPPORT is continuously monitoring and patching the security vulnerability.

Data Transfer through Secured Channel

A lot of works using computers are stored on local computers or online via Internet. This data needs secured channel to be transferred.

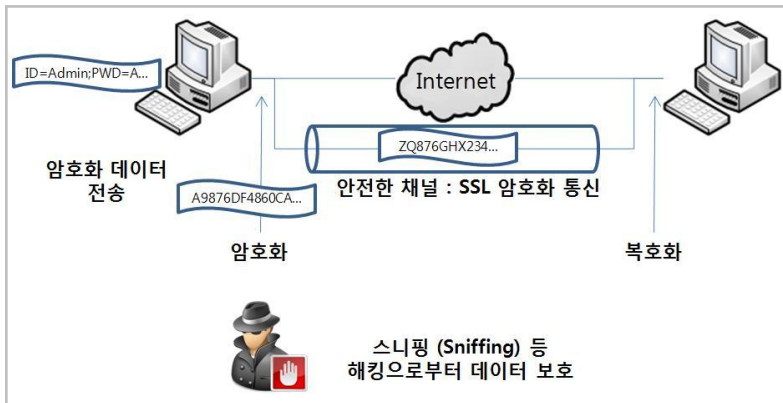
Transferring unencrypted Plain text data can be sniffed by hackers any time.

Image 3 Data exposure by sniffing



To transfer secure data and protect it from hackers, Data should be encrypted on local computer first and use encrypted channel such as SSL(Secure Socket Layer) to send it over the network.

Image 4 Data protection from hacking like sniffing



Data below should be protected while remote supporting.
Screen Sharing, Keyboard/Mouse control, Text Chat, File Transfer, Created Data by remote support functions

RSUPPORT's products support 256-bit AES encryption from end to end as a first security process. Then 128-bit SSL (Secure Socket Layer) is involved during the remote session as a second security process.

Grid Server security at Data center

RSUPPORT is operating and managing Grid servers in the Data center over the world.

RSUPPORT has grid servers in Korea, Japan, USA and Singapore currently. Each data center is managed and operated by local staff 24/7 and they are secured by biometrics entrance security systems. Grid Servers support Failover without any downtime.

Web Server security

RSUPPORT security servers load SSL web server certificate issued by Thawte(www.thawte.com). This enables to provide secure 128-bit SSL (Secure Sockets Layer) encryption during remote support.

With using SSL (Secure Sockets Layer) Web server, All data and information between PC and server can be secured and transferred with giving unbreakable data for sniffing attacks.

Encrypted Communication support

Every support sessions use 128bit SSL (Secure Socket Layer) encryption.

End-To-End Data protection

Every support sessions use End-To-End 128-bit AES (Advanced Encryption Standard) encryption for transferred data.

Support page(startsupport.com, rsup.net) security

Every support sessions don't display other user's remote support list on support page such as startsupport.com or rsup.net

Connection code security

Connection code for remote support authorization provides 6 to 9 digit number randomly generated. Generated connection code is disposed after remote support is connected. No one can access the same session with this disposable connection code.

Secure HTTP(HTTPS)

Support page uses HTTPS. Users can have safe web access through HTTPS. HTTPS uses 443 Port to communicate.

Digital signature and Code signing for remote support module

RSUPPORT uses digitally signed or code signed ActiveX or Executable files which are digitally signed or code signed by Verisign

Non ActiveX remote support

RSUPPORT also provides non ActiveX remote support products. These products can initiate support or screen sharing through Chat and this doesn't require any installation of ActiveX. (RemoteCall v4.0 needs to install ActiveX to support.)

No Pre-installed Software

Customers is able to get support via an Internet browser without installing any program.

Security equipment

RSUPPORT's products are completely compatible with Security equipment such as Firewall, IPS, HTTP Proxy. They use port 80 for HTTP and use port 443 for HTTPS. In most cases, Port 443 and 80 are available to end users since these 2 ports are network standards.

User Approval requirement before remote support

Customer must authorize representative to share desktop before getting remote support.

User Approval for Keyboard/Mouse control

Mouse/Keyboard needs to be approved to proceed by users before remote support begins. Customer can gain Keyboard/Mouse control again any time during the remote support session with pressing "Ctrl + Alt + Shift" together.

User Approval for File Transfer

File Transfer also needs to be approved to proceed by users. Any unintended file transfer is restricted without customer's authorization.

Notification for Remote support session

There are 2 ways to show messages of remote support status. One is a connection status window that shows connection information and Users can disconnect the session any time by clicking "disconnect" button in the window. Another one is the message on the right-bottom of the desktop showing "Screen Sharing...". Users can see remote support is in process.

History Logging

Chat and File transfer history leaves logs and they are saved/managed in the Server. Remote support session recording ensures safe remote support for both users and representatives.

Indirect control for Remote support

Laser pointer, Drawing enables representative to remote support indirectly. This indirect remote support makes users feel more comfortable about remote support.

URL push is one of indirect remote support features by directing users to visit a website.

Zero footprint after remote support

User can remove all remote support module after remote support.

Permissions for representative's control

RSUPPORT products provide Administrator with Permission settings at Admin Center webpage.

Also Administrator can restrict representatives' control by group.

Network restriction

Network access restrictions are provided for Administrator to configure restrictions representative's network. Administrator can add restricted IP address or MAC address into list then representative should log in to Agent within the permitted range.

Appendix

SSL (Secure Socket Layer)

SSL is in between Application protocol and TCP/IP and provides Data encryption, Server authentication, Integrity of messages. Authentication for server has to be performed but Authentication for clients is optional.

SSL performs handshake protocol to connect server and client with TCP/IP. This results in bilateral encryption correspondence and prepares the necessary values for encryption correspondence and authentication.

After this step, SSL performs encryption and decryption of the Bytes that Application protocol generates. This means all information includes HTTP Request and HTTP Response is encrypted and transferred.

AES (Advanced Encryption Standard)

AES(Advanced Encryption Standard) is a encryption that US Government has adopted in 2001. AES provides much secured encryption than DES(Data Encryption Standard) or 3DES.

Contact Information

RSUPPORT: www.rsupport.com

Technical Support: support@rsupport.com

Sales: sales@rsupport.com

Info: info@rsupport.com

Headquarters:

Nano Bldg., 149-11,
Bangi-dong, Songpa-gu,
Seoul, Korea
Phone: +82-70-7011-0590
Fax: +82-2-479-4429

USA Office:

116 West 23rd Street, Suite 500,
New York, NY 10011,
USA
Phone : +1-888-348-6330
Fax : +1-888-348-6340

China Office:

Rm1903 block4No.5
Changchunqiao Road,
Haidian District, Beijing 100089, China
Phone : +86-10-8256-1810
Fax : +86-10-8256-2978

Japan Office:

Shinkasumigaseki Bldg., 18F, 3-3-2,
Kasumigaseki, Chiyoda-ku,
Tokyo 100-0013, Japan
Phone : +81-3-3539-5761
Fax: +81-3-3539-5762